Deutscher Bundestag
11. Wahlperiode

Drucksache 11/6458

14. 02. 90

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Zwölfter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz vom 14. Februar 1990 — I — 111/14 — gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes.

1 Überblick über das Berichtsjahr

1.1 Einleitung

1.1.1 Gesamtpolitische Entwicklung

Der Datenschutz steht für einen wichtigen Teil unserer freiheitlichen Ordnung. Es ist erfreulich, heute feststellen zu können, daß auch die Menschen in Ost- und Mitteleuropa im Datenschutz ein wichtiges Element ihrer politischen Neuorientierung erkennen. So kündigte auf der Internationalen Datenschutzkonferenz Ende August 1989 in Berlin ein Teilnehmer aus Ungarn unter dem Beifall aller Konferenzteilnehmer an, sein Land werde demnächst nicht nur der Datenschutzkonvention des Europarates beitreten, sondern das Recht auf Datenschutz auch in der neuen Ungarischen Verfassung verankern. Im gleichen Sinn bezeichnete eine polnische Journalistendelegation, die meine Dienststelle vor einiger Zeit besuchte, den Datenschutz als essentiellen Teil einer Demokratie. Dies verwundert nicht. Menschen, die in einer Gesellschaftsordnung leben, wo immer und überall mit Überwachung durch im Geheimen arbeitende Dienste zu rechnen ist, wissen am besten, wie wichtig es ist, die Beschaffung und Verwertung personenbezogener Daten über sie transparent zu machen und zu kontrollieren.

Unsere Rechtsordnung geht zu Recht nicht von einem Menschen ohne Schwächen und Fehler aus. Wir betrachten es auch nicht als Aufgabe des Staates, den Menschen so lange umzuerziehen, bis er dieses Idealbild erreicht hat. Aber weil wir die menschlichen Schwächen und Fehler kennen, legen wir großen Wert auf ein wirksamens System von Vorkehrungen und Kontrollen gegen den Mißbrauch von Befugnissen und gegen den exzessiven Gebrauch von Macht. Die Datenschutzkontrolle ist die jüngste Ausprägung dieses Gedankens. Sie soll dazu beitragen, das Grundrecht auf freie Entfaltung der Persönlichkeit zu schützen. Sie wurde in dem Bewußtsein geschaffen, daß der Bürger eine vom Staat und auch von anderen Menschen zu respektierende Privatsphäre braucht, und weil wir der Auffassung sind, daß der einzelne grundsätzlich selbst entscheiden können soll, welche Informationen über ihn selbst andere besitzen sollen. Der Datenschutz ist zugleich eine Antwort auf die Herausforderungen der modernen Informationstechnik. Da diese sich rasant fortentwickelt, darf auch der Datenschutz, der diese Risiken beherrschbar machen soll, nicht auf der Stelle treten.

1.1.2 Innerdeutsche Entwicklung

Die politische Entwicklung in Mittel- und Osteuropa hat sich in besonderer Weise auf das Verhältnis zwischen den beiden deutschen Staaten ausgewirkt. Schon jetzt zeigt sich eine vermehrte Zusammenarbeit zwischen öffentlichen und privaten Stellen der Bundesrepublik Deutschland und solchen der Deutschen Demokratischen Republik, die aller Voraussicht nach schon sehr bald noch ganz erheblich zunehmen wird. Diese Entwicklung führt zwangsläufig auch zu einem vermehrtem Austausch personenbezogener Daten. Gegen Ende 1989 haben beispielsweise erste deutsch-deutsche Gespräche über eine polizeiliche Zusammenarbeit auf dem Gebiet der Rauschgiftbekämpfung stattgefunden. Auch eine innerdeutsche Zusammenarbeit auf dem Gebiet der Sozialversicherung, insbesondere zur Bekämpfung von Schwarzarbeit und zur Verhinderung von Leistungsmißbrauch wird angestrebt. Andere Bereiche der öffentlichen Verwaltung werden sicher folgen. Die damit verbundenen datenschutzrechtlichen Implikationen sind für die Betroffenen von erheblicher praktischer Bedeutung. Dies gilt insbesondere deshalb, weil es in der DDR einen Datenschutz in unserem Sinn praktisch nicht gibt. Angesichts der besonderen Lage wird dennoch niemand verlangen, daß die DDR als Vorbedingung für den Austausch personenbezogener Daten ein komplettes Datenschutzmodell vorweisen muß. Andererseits kann angesichts der besonderen Qualität und Intensität der angestrebten Zusammenarbeit der Datenschutz nicht einfach ausgeklammert werden. Ich habe deshalb empfohlen, die Fragen des Datenschutzes von Anfang an in die deutsch-deutschen Verhandlungen einzubeziehen. Denn die ersten Vereinbarungen mit der DDR über die gegenseitige Zusammenarbeit, in denen ein Austausch oder eine sonstige Verarbeitung personenbezogener Daten vorgesehen wird, werden wesentlich für den datenschutzrechtlichen Standard sein, der in Zukunft bei der innerdeutschen Zusammenarbeit angewandt wird.

1.1.3 Europäische Gemeinschaft

Im Berichtsjahr hat die Bedeutung des Datenschutzes im internationalen Bereich, insbesondere aber für das Gebiet der Europäischen Gemeinschaft, erheblich zugenommen. Das wird schon dadurch dokumentiert, daß von den insgesamt acht Entschließungen, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz 1989 gefaßt hat, allein drei europäische Probleme zum Gegenstand haben (s. Anlagen 6, 8 und 9).

Die größte aktuelle Bedeutung hat das sog. Schengener Übereinkommen, mit dem sich Frankreich, die Benelux-Länder und die Bundesrepublik Deutschland verpflichtet haben, die Grenzkontrollen zwischen diesen Ländern schrittweise abzubauen. Um Sicherheitsdefizite zu vermeiden, soll gleichzeitig die Zusammenarbeit der Behörden der beteiligten Staaten verbessert werden, so etwa auf den Gebieten der Kontrollen an den Außengrenzen, der polizeilichen Gefahrenabwehr, der Strafverfolgung, des Ausländerrechts, des Asylverfahrens, der Bekämpfung des Betäubungsmittelmißbrauchs und des Waffenrechts. Welche zentrale Bedeutung dabei dem Datenschutz zukommt, zeigt eindrucksvoll der Entwurf des diese Zusammenarbeit regelnden Zusatzübereinkommens zum Schengener Übereinkommen. Es enthält für einen großen Bereich datenschutzrechtlich gute Regelungen, läßt aber insgesamt doch noch einige Wünsche offen, worauf die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hingewiesen hat (s. 27.6 sowie Anlage 6).

Mit dem grenzüberschreitenden Datenverkehr, dessen Bedeutung insbesondere als Folge des europäischen Binnenmarktes erheblich anwachsen wird, haben sich sowohl die Internationale Datenschutzkonferenz in Berlin als auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz befaßt. In den von beiden Gremien erarbeiteten Entschließungen (s. Anlagen 8 und 12) wird dringend gefordert, innerhalb Europas ein möglichst einheitliches Datenschutzrecht auf hohem Niveau zu schaffen. Beide Konferenzen haben ihrer Sorge Ausdruck gegeben, daß zwar die technischen und organisatorischen Voraussetzungen für die internationale Datenübermittlung immer weiter verbessert werden — z. B. durch die schon 1992 zu erwartende europaweite Einführung von ISDN —, der Entwicklung des Datenschutzes aber nicht die gleiche Priorität gegeben wird. Besonders beklagt wurde, daß gerade die Europäische Gemeinschaft sich durch eine große Enthaltsamkeit auf dem Gebiet des Datenschutzes auszeichnet, obwohl mit dem europäischen Binnenmarkt ein informationeller Großraum von 320 Mio. Menschen geschaffen wird. Es ist deshalb notwendig, daß die Europäischen Gemeinschaft die Bedeutung des Datenschutzes erkennt und bald entsprechende praktische Konsequenzen zieht (s. 27.3).

1.1.4 Technische Entwicklung

Der technisch-industriell bedeutsame Wissensstand verdoppelt sich derzeit nach ernstzunehmenden Angaben in einem Zeitraum von etwa 5 bis 6 Jahren. Von besonderer Bedeutung ist dabei die Entwicklung von Techniken zur Verarbeitung und Verbreitung von Informationen in der zweiten Hälfte unseres Jahrhunderts. Diese Entwicklung hat dazu geführt, daß sich unsere moderne Industriegesellschaft bereits auf dem Weg in eine Informations- und Kommunikationsgesellschaft befindet, in der Information neben Arbeit, Boden und Kapital zunehmend zum vierten Produktionsfaktor wird. Die Möglichkeiten zur Beschaffung, Aufzeichnung, Verknüpfung und Auswertung von Informationen sind in einem vor kurzem noch unvorstellbaren Ausmaß gewachsen. Die Abschnitte dieses Berichtes zu den Bereichen Post und Telekommunikation sowie Datensicherung (s. 7 und 24), die nur einen sehr kleinen Teil von Telekommunikationstechnik ansprechen, zeigen, welche unterschiedlichen Möglichkeiten sich in unserer Zeit für Kommunikation und Datenverarbeitung ergeben haben.

Mit der Zunahme der Angebote moderner Technik für Telekommunikation und Datenverarbeitung wachsen freilich auch die Risiken für den privaten Freiraum des Bürgers, den unsere Rechts- und Gesellschaftsordnung mit Recht als hohes Gut bewertet. Das flüchtig gesprochene Wort und andere Tatsachen über ein vertraulich geführtes Gespräch oder sonstige Informationen können heute völlig problemlos und preisgünstig festgehalten, verarbeitet und genutzt werden. Die neue Technik läßt auch das Problem der Funktions- und Datensicherung, z. B. bei der Identifizierung des Kommunikationspartners entstehen. Bei den traditionellen Kommunikationsmitteln bereits bekannte Schwächen für Funktions- und Datensicherheit erhalten bei den neuen Techniken erheblich größeres Gewicht. Aus all diesen Gründen muß das Bemühen zunehmen, bei der Anwendung neuer Informationstechniken mehr Datenschutz und auch mehr technische Sicherheit zu erreichen. Diese Forderung ist letztlich aus dem Grundsatz abzuleiten, daß die neuen Informationstechniken — wie jede andere Technik auch — nur unter Beachtung ethischer Prinzipien und von Grundnormen unserer Rechtsordnung angewendet werden dürfen.

Bei dem Versuch, eine Antwort auf diese Herausforderung zu finden, darf die Sensibilität unserer Bürger gerade für diesen Bereich der modernen gesellschaftlichen Entwicklung nicht übersehen werden. Wenn die neuen Informationstechniken und ihre Anwendung akzeptiert werden sollen, ist eine Vertrauenswerbung dafür notwendig. Unserer Bevölkerung muß überzeugend dargelegt werden können, daß der Staat bei der Einführung der neuen Techniken und bei der Festlegung der Normen für den Umgang mit ihnen nicht nur den damit verbundenen Fortschritt an ökonomischer Effizienz und Erleichterung der Arbeit, sondern auch den notwendigen Schutz der Privatsphäre der Bürger beachtet. Dazu könnte beitragen, den Bundesbeauftragten für den Datenschutz rechtzeitig vor der Einführung solcher Techniken und der Festlegung der Normen für den Umgang mit ihnen zu beteiligen, wie es der Bundestag in seinem Beschluß zu meinem Sechsten und Siebenten Tätigkeitsbericht — Drucksache 10/6583 — gefordert hat. Bei der Erarbeitung der Konzeption für ISDN war das leider nicht der Fall.

Der Vertrauenswerbung würde es auch dienen, wenn gerade die öffentliche Verwaltung bei der Anwendung neuer Techniken den Schutz personenbezogener Daten stets mit besonderer Sorgfalt achten und die dafür geltenden Vorschriften peinlich genau einhalten würde. Aber gerade in diesem Bereich ist noch manches zu verbessern. Das zeigt die Zusammenstellung der Beanstandungen (s. 1.3), die zu einem guten Teil Fälle ausweist, die mit dem Einsatz von Informationstechnik zusammenhängen. Es dient z. B. nicht der Akzeptanz dieser Technik, wenn in einem Bundesministerium der Einsatz von Arbeitsplatzcomputern ungeplant und unkontrolliert erfolgt, wenn die Deutsche Bundespost bei ISDN Verbindungsdaten im Widerspruch zu den Vorschriften der Telekommunikationsordnung aufzeichnet, und wenn weder das Bundeskriminalamt noch das Kraftfahrtbundesamt erkennen, daß bestimmte Schaltungen von Online-Verbindungen und die dadurch ermöglichten Abrufe personenbezogener Daten nach den klaren Vorschriften des Straßenverkehrsgesetzes untersagt waren.

Der Datenschutz tritt der Fortentwicklung und dem Einsatz moderner Informationstechnik nicht feindlich entgegen. Was er fordert, ist, daß der Einsatz dieser Technik ethisch verantwortbar und in einer Weise erfolgt, die mit den Grundnormen unserer Verfassung übereinstimmt sowie das Recht unserer Bürger auf Schutz ihrer Privatsphäre im größtmöglichen Umfang gewährleistet.

1.1.5 Datenschutzrechtlich bedeutsame Gesetzgebung

Die Erwartung, 1989 könne im Bundesbereich ein entscheidendes Jahr zur Verbesserung des Datenschutzes werden, hat sich leider nicht erfüllt. Zu dem von der Bundesregierung Ende 1988 vorgelegten Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes hat der Bundesrat eine große Zahl begrüßenswerter Änderungsvorschläge gemacht. In einer vom Innenausschuß des Deutschen Bundestages durchgeführten öffentlichen Anhörung habe ich zu dem Entwurf des Bundesdatenschutzgesetzes und zu der im Zusammenhang damit vorgesehenen Ergänzung des Verwaltungsverfahrensgesetzes Stellung genommen. In einer zweiten Anhörung hatte ich Gelegenheit, meine Bewertung der im gleichen Gesetzentwurf vorgesehenen Neufassung des Verfassungsschutzgesetzes sowie der Entwürfe eines MAD- und eines BND-Gesetzes vorzutragen. Dabei habe ich die Positionen vertreten, die ich auch im 11. Tätigkeitsbericht (s. 25.1 und 19.1) eingenommen habe; diese entsprechen in allen wesentlichen Punkten den Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (s. Anlagen 1 und 5). Die zuständigen Ausschüsse des Bundestages haben den vorerwähnten Gesetzentwurf bisher noch nicht eingehend beraten. Ich bitte erneut dringend darum, den Gesetzentwurf soweit irgendmöglich zu verbessern und noch in dieser Legislaturperiode zu verabschieden. Die Bürgerinnen und Bürger unseres Landes brauchen möglichst rasch Sicherheit über ihre Rechte auf dem Gebiet des Datenschutzes. Auch die Behörden und die Wirtschaft müssen so schnell wie möglich Klarheit über den Umgang mit personenbezogenen Daten erhalten. Es wäre tief zu beklagen, wenn mehr als sechs Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts nicht die grundsätzlichen gesetzgeberischen Konsequenzen aus dem Urteil gezogen würden.

Ein datenschutzrechtlich bedeutsames Gesetz, mit dem ich mich zu befassen hatte, war das Poststrukturgesetz. Bei der im Laufe des Gesetzgebungsverfahrens durchgeführten Beratung des Deutschen Bundestages und der Bundesregierung konnten zwar nicht alle wünschenswerten Detaillierungen erreicht werden; insgesamt bieten aber die datenschutzrechtlich bedeutsamen Vorschriften des Gesetzes eine geeignete Grundlage für eine angemessene Regelung der anstehenden Datenschutzprobleme sowohl im öffentlichen wie im privaten Bereich. Es kommt jetzt darauf an, daß die im Gesetz vorgesehenen Rechtsverordnungen, mit denen bereichsspezifische Regelungen geschaffen werden sollen, gute Lösungen enthalten.

Auch im Gesetz über die Einführung des Sozialversicherungsausweises konnten im Laufe des Gesetzgebungsverfahrens noch zusätzliche datenschutzrechtliche Regelungen verankert werden, die die mit der Verwendung des Sozialversicherungsausweises verbundenen datenschutzrechtlichen Fragen angemessen lösen.

Erfreulich war auch, daß in das Rentenreformgesetz ein eigener Abschnitt über den Datenschutz eingefügt wurde, der erheblich mehr Klarheit über den bei der Verarbeitung personenbezogener Daten in der Rentenversicherung zu gewährleistenden Datenschutz gibt.

Diese Ergebnisse zeigen, daß der Gesetzgeber die Anforderungen einer modernen Verwaltung sehr wohl mit den Notwendigkeiten des Datenschutzes in Einklang bringen kann. Dem Bundesminister für Arbeit und Sozialordnung möchte ich in diesem Zusammenhang für die gerade bei den letztgenannten Gesetzentwürfen gezeigte kooperative Haltung danken.

1.1.6 Die Beratungsaufgabe des Bundesbeauftragten für den Datenschutz

Angesichts des großen Umfangs der Gesetzgebung und sonstigen Rechtsetzung des Bundes kommt meiner in § 19 Abs.1 Satz 2 BDSG vorgesehenen Beratungsaufgabe eine hohe Bedeutung zu. Diese nimmt meine Dienststelle in hohem Maße in Anspruch. Nicht selten ergeben sich bei der Beratung Probleme, weil meine Beteiligung an den Entwürfen entsprechender Rechtsvorschriften nicht, wie es der Deutsche Bundestag in der Drucksache 9/1623 gefordert hat, „möglichst frühzeitig" erfolgt. Fällen mit vorbildlicher und recht früher Beteiligung — etwa bei den Entwürfen der Gesetze zum Ausländerzentralregister und zum Ausländerrecht sowie beim Entwurf des Strafverfahrensänderungsgesetzes — stehen solche gegenüber, bei denen eine Beteiligung überhaupt nicht oder zu spät erfolgte. So wurde ich z. B. bei der Erarbeitung des Entwurfs eines Verbraucherkreditgesetzes nicht beteiligt, obwohl ich in meinem 11. Tätigkeitsbericht auf das sich dabei ergebende datenschutzrechtliche Grundproblem hingewiesen hatte. Von manchen Entwürfen von Gesetzen oder anderen Rechtsvorschriften erfahre ich erst im Zusammenhang mit der Verteilung der Drucksachen des Deutschen Bundestages. Ich bitte noch einmal dringend darum, mich bei der Vorbereitung datenschutzrechtlich bedeutsamer Regelungen möglichst frühzeitig zu beteiligen. Dies wäre die beste Gewähr dafür, datenschutzrechtliche Erfordernisse bereits bei der Ausarbeitung von Gesetzentwürfen zu erkennen und die sich daraus ergebenden Fragen durch entsprechende Vorschriften in den Entwürfen zu lösen.

Während die Beteiligung im Bereich der Bundesregierung teilweise zu wünschen übrig läßt, ist meine Zusammenarbeit mit dem Deutschen Bundestag erfreulich gut. Ich werde dort fast ausnahmslos mit meinen Anliegen gehört und finde in den allermeisten Fällen auch Verständnis für meine Aufgabe. Ich würde es allerdings begrüßen, wenn es in Zukunft gelänge, meine Tätigkeitsberichte im Bundestag früher zu beraten. Die Tätigkeitsberichte enthalten unter anderem eine Darstellung meiner Beanstandungen und weisen auf datenschutzrechtliche Probleme hin, über die kein Einvernehmen mit der Bundesregierung erzielt werden konnte. In diesen Fällen besteht häufig die einzige Möglichkeit, die datenschutzrechtlichen Belange unserer Bürger zu wahren, darin, daß der Deutsche Bundestag bei der Beratung meiner Berichte die ausgesprochenen Beanstandungen und die dargestellten Probleme politisch erörtert und, soweit er sich meiner

Auffassung anschließt, entsprechende Forderungen gegenüber der Bundesregierung erhebt. Dieses Verfahren ist umso wirksamer je zügiger die Beratung der Tätigkeitsberichte erfolgt. Mir ist natürlich bekannt, wie belastet die zuständigen Ausschüssse des Deutschen Bundestages sind. Gleichwohl muß ich darauf hinweisen, daß es mit der Wahrung der Rechte unserer Bürger nur schwer vereinbar ist, wenn im Januar 1990 die Datenschutzberichte für die Jahre 1987 und 1988 noch nicht im Bundestag beraten worden sind.

1.1.7 Eingaben von Bürgerinnen und Bürgern

Sinn des Datenschutzes ist nicht die Durchsetzung abstrakter datenschutzrechtlicher Grundsätze, sondern der praktische Schutz der Privatsphäre der Bürger, insbesondere ihrer personenbezogenen Daten. Ein datenschutzrechtliches Engagement, das nicht auf diese Wirkung zielte, wäre hohl und schal und letztlich nicht gerechtfertigt. Ein guter Indikator dafür, wo Datenschutz geboten ist und wo es noch datenschutzrechtliche Defizite zu bereinigen gilt, sind die an mich gerichteten Eingaben von Bürgerinnen und Bürgern. Nach § 21 BDSG kann sich jedermann an den Bundesbeauftragten für den Datenschutz wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Behörden oder sonstige öffentliche Stellen des Bundes in seinen Rechten verletzt worden zu sein.

Die Eingaben der Bürger betreffen nahezu alle Bereiche der Bundesverwaltung. Zahlenmäßig im Vordergrund stehen die Sozialversicherung, insbesondere die Arbeitslosenversicherung, gefolgt von der Deutschen Bundespost und den Sicherheitsbehörden.

In nicht wenigen Fällen gelingt es mir, dem einzelnen Bürger zu seinem Recht zu verhelfen. So konnte ich z. B. erreichen, daß

- ein Petent, gegen den ein Ermittlungsverfahren eingeleitet, aber später eingestellt worden war, über seine fortbestehende Speicherung in einer regionalen Täterkartei des Fahndungsdienstes der Deutschen Bundesbahn und in der sogenannten Schwarzfahrerdatei unterrichtet wurde
- ein begeisterter Segelflieger, dem die Fluglizenz aus medizinischen Gründen entzogen worden war, Einsicht in ein ihm bis dahin vorenthaltenes für ihn positives ärztliches Gutachten erhielt
- die Daten eines Bürgers, die nur deshalb in einem Computer des Verfassungsschutzes gespeichert worden waren, weil er einmal zur Unterstützung der Spionageabwehrbehörden Angaben gemacht hatte, gelöscht wurden
- die Bewertung einer Tätigkeit eines Bundesbeamten aus den Jahren 1972 bis 1974 auf der Grundlage der neuen Sicherheitsrichtlinien noch einmal mit dem Ergebnis überprüft wurde, daß Bedenken gegen eine Verwendung des Beamten im sicherheitsempfindlichen Bereich nicht mehr erhoben wurden.

Manche Eingaben führen dazu, daß nach meiner Intervention ganze Verwaltungsverfahren geändert werden. So hat z. B.

- der Bundesminister der Finanzen angeordnet, daß bei der Abfertigung von geringwertigem Umzugsgut von Aussiedlern nur noch eine mündliche — keine schriftliche — Zollanmeldung erfolgen muß, und auch keine schriftliche Abfertigung dieses Gutes „zum freien Verkehr" mehr ausgestellt wird, wodurch in diesen Fällen auch die bisher praktizierte 10jährige Aufbewahrung des Abfertigungsbescheides bei den Hauptzollämtern entfällt
- ein Sozialversicherungsträger sein Verfahren zur Vernichtung von Computerausdrucken neu geregelt und damit für die Zukunft verhindert, daß solche Schriftstücke — wie geschehen — in Müllcontainern gefunden werden.

In manchen Fällen ist es mir nicht gelungen, eine bürgerfreundliche Regelung zu erreichen, obwohl dies notwendig wäre. So hat sich der Bundesminister für Post und Telekommunikation bisher nicht bereit gefunden, die in einer Eingabe kritisierte und auch nach meiner Überzeugung nach geltendem Recht unzulässige Praxis der Deutschen Bundespost aufzugeben, anfragenden Dritten, die nur die Nummer des Postfaches eines Kunden kennen, auch dessen vollständige Anschrift mitzuteilen.

Die Deutsche Bundespost — Telekom hat bisher leider auch noch nichts an der mit der Telekommunikationsordnung unvereinbaren Praxis der Datenspeicherung bei Mobilfunk und ISDN geändert, gegen die sich Eingaben von Bürgern und besonders von Mitarbeitern der Telefonseelsorge gewandt haben.

Natürlich sind nicht alle Eingaben von Bürgern begründet. In solchen Fällen versuche ich die Petenten davon zu überzeugen, daß und warum die Verwaltung richtig gehandelt hat. So konnte ich z. B. dem Mieter eines in Eigentum des Bundes stehenden Mietshauses, der die Streupflicht für die Straße vor dem Haus übernommen hatte, erläutern, warum das Bundesvermögensamt nicht gegen den Datenschutz verstieß, als es seinen Namen einem Dritten mitteilte, der begründet dargelegt hatte, daß er infolge Verletzung der Streupflicht einen Schaden erlitten hatte.

Ganz vereinzelt erreichen mich auch Beschwerden, die sich gegen ihrer Meinung nach unberechtigten und übertriebenen Datenschutz wenden. Auch den Anliegen dieser Bürger gehe ich mit großer Sorgfalt nach, weil Datenschutz ja nicht dazu dienen darf, Bürgern ungerechtfertigte Schwierigkeiten oder Nachteile zu bereiten. Ein Beispiel dafür ist die Familienforschung. Seit Jahren schreiben mir Bürger, daß § 61 Abs. 1 des geltenden Personenstandsgesetzes sie an der Familienforschung hindere, weil er fordere, daß Personen, die nicht Abkömmlinge der Person sind, nach der geforscht werden soll, ein „rechtliches Interesse" an der Auskunft darlegen müssen. Ich teile in dieser Frage die Ansicht der Bürger und habe dem BMI empfohlen, die geltende Regelung dahin zu ergänzen, daß die Glaubhaftmachung eines „berechtigten Interesses" genügt, wenn seit dem Tod des Betroffenen mindestens 30 Jahre oder seit seiner Geburt 120 Jahre vergangen sind.

1.1.8 Datenschutzrechtliche Kontrollen

Die Kontrollen von Bundesbehörden durch meine Dienstelle werden zu einem großen Teil aufgrund eines zu Beginn des Berichtsjahres erstellten Arbeitsplanes durchgeführt. Bei dessen Erstellung werden vorhandene Anhaltspunkte für mögliche Verstöße gegen datenschutzrechtliche Vorschriften aus den Vorjahren berücksichtigt. Häufig veranlassen mich aber auch Eingaben von Bürgern oder die Einführung neuer Datenverarbeitungen oder auch neue Rechtsvorschriften zu Kontrollmaßnahmen. Gelegentlich wird mit einer Kontrolle aber einfach angestrebt, einen bisher noch nicht geprüften Bereich näher kennenzulernen.

Die datenschutzrechtliche Kontrolle ist ein unverzichtbares Instrument zur Durchsetzung eines wirksamen Datenschutzes. Dabei ist es nie das Ziel, eine Behörde „anzuschwärzen". Ziel muß immer sein, möglichst effektiven Datenschutz für die Bürger zu erreichen. Der immer mehr zunehmende Einsatz automatisierter Datenverarbeitung führt dazu, daß die Prüfung von Verfahren der automatisierten Datenverarbeitung bei den Kontrollen immer größere Bedeutung erlangt. Die Kontrollen führen nicht selten zu förmlichen Beanstandungen nach § 20 BDSG. Zum überwiegenden Teil enden sie aber — das ist erfreulich — lediglich mit Empfehlungen für weitere Verbesserungen des Datenschutzes, die in aller Regel von den Behörden dankbar akzeptiert werden.

1.1.9 Zusammenfassung

Dieser Bericht erhält Erfreuliches und Tadelnswertes. Erfreulich ist vor allem die hohe Akzeptanz des Datenschutzes im Bereich der Politik, insbesondere bei den Abgeordneten des Deutschen Bundestages. Im Zuge der Beratung von Gesetzentwürfen kann ich immer wieder deutliche datenschutzrechtliche Verbesserungen an Regierungsvorlagen erreichen. Allerdings fielen auch im politischen Bereich vereinzelt Äußerungen, die auf wenig Verständnis für den Datenschutz schließen lassen. So wurde z. B. nach dem furchtbaren Terroranschlag auf den Sprecher der Deutschen Bank Herrhausen im Zusammenhang mit den aufgrund dieses Ereignisses zu treffenden Maßnahmen gefordert, die Datenschutzvorschriften zu überprüfen, weil Datenschutz nicht zum Täterschutz werden dürfe. Dies geschah, obwohl nach der eindeutigen Sachlage nicht der mindeste Anhaltspunkt dafür bestand, daß der Anschlag bei weniger Datenschutz hätte verhindert werden können

Auch im Bereich der Verwaltung stehen einem deutlich sichtbaren Streben nach Gewährleistung eines guten Datenschutzstandards, für das besonders den Datenschutzbeauftragten der Behörden zu danken ist, gelegentlich eine Blickverengung nur auf die Erfüllung der eigenen Aufgaben, ein geringes Maß an Sensibilität für die Belange des Datenschutzes und wenig Verständnis für das Amt des Bundesbeauftragten für den Datenschutz gegenüber. Der Datenschutz ist zwar weitgehend akzeptiert, vielfach aber noch nicht so selbstverständlich wie es eigentlich sein müßte. Unabhängige Datenschutzkontrolle ist weiter erforderlich. Dies nicht deshalb, weil die Bediensteten in unseren Behörden grundsätzlich gegen den Datenschutz eingestellt sind, sondern weil Datenschutz in aller Regel mehr Aufmerksamkeit, zusätzliche Anstrengung und vermehrten Aufwand fordert, und weil jedes menschliche Tun mit der realen Möglichkeit des Fehlers behaftet ist. Daran wird sich, weil es offenbar zur Natur des Menschen gehört, auch in Zukunft nichts ändern. Datenschutz muß deshalb immer wieder zum Schutz der Privatsphäre unserer Bürger auf Schwächen von Verfahren und Einrichtungen der Datenverarbeitung, unzureichende rechtliche Regelungen, offenkundige Mängel und Rechtsverstöße hinweisen. Mit den ausgesprochenen Beanstandungen und Empfehlungen leistet er einen Beitrag dafür, daß unsere Rechts- und Gesellschaftsordnung freiheitlich und menschenwürdig bleibt.

1.2 Kontrollen und Beratungen

Bei folgenden Behörden haben Mitarbeiter meiner Dienststelle im Berichtsjahr Kontrollen, Beratungen oder Informationsbesuche durchgeführt:

Verwaltung des Deutschen Bundestages

Bundeskanzleramt

Auswärtiges Amt

Bundesminister des Innern

Bundesminister der Justiz

Bundesminister der Finanzen

Bundesminister für Arbeit und Sozialordnung

Bundesminister der Verteidigung

Bundesminister für Jugend, Familie, Frauen und Gesundheit

Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit

Bundesminister für Post und Telekommunikation

Bundesminister für wirtschaftliche Zusammenarbeit

Bundesrechnungshof

Botschaft Ankara

Generalkonsulat Istanbul

Bundesverwaltungsamt

Bundesamt für Verfassungsschutz

Bundeskriminalamt

Bundeszentralregister

Bundesaufsichtsamt für das Kreditwesen

Bundesamt für Wirtschaft

Bundesanstalt für Arbeit

drei Arbeitsämter

Streitkräfteamt

Akademie für psychologische Verteidigung der Bundeswehr

Bundesgesundheitsamt

Deutsche Bundesbahn

Bundesanstalt für Straßenwesen

Kraftfahrt-Bundesamt

Bundesanstalt für Flugsicherung

Umweltbundesamt

Bundesdruckerei

ein Postgiroamt

fünf Fernmeldeämter

Verband Deutscher Rentenversicherungsträger — Datenstelle —

Verband der Angestellten-Ersatzkassen

Bundesverband der Betriebskrankenkassen

Betriebskrankenkasse des Bundesministers für Verkehr

Kaufmännische Krankenkasse Hannover

Versorgungsanstalt der Deutschen Bundespost

Versorgungsanstalten der Deutschen Bühnen und der Deutschen Kulturorchester bei der Bayerischen Versicherungskammer

Maschinenbau-Berufsgenossenschaft

See-Berufsgenossenschaft/Seekasse

Nachfolgend sind wichtige aktuelle Themen und die Art ihrer Bearbeitung aufgeführt:

Thema	**Art der Erledigung**
Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes (Neufassung des Bundesdatenschutzgesetzes, Änderung des Verwaltungsverfahrensgesetzes, Neufassung des Bundesverfassungsschutzgesetzes, MAD-Gesetz, BND-Gesetz)	— Anhörungen im Innenausschuß des Deutschen Bundestages mit schriftlicher Stellungnahme — Anhörung durch die Arbeitsgruppe Inneres der CDU/CSU-Fraktion des Deutschen Bundestages und schriftliche Stellungnahme — Anhörung durch den Arbeitskreis II der SPD-Fraktion des Deutschen Bundestages und schriftliche Stellungnahme
Novellierung der Rechtsgrundlagen für Einzelstatistiken, u. a. zu den Entwürfen eines — Rohstoffstatistikgesetzes, — Handwerksstatistikgesetzes, — Mikrozensusgesetzes, — Gebäude- und Wohnungsstichprobengesetzes, — Strafverfolgungsstatistikgesetzes	Beratung und schriftliche Stellungnahmen gegenüber Ausschüssen des Deutschen Bundestages und den zuständigen Bundesministerien
Entwurf eines Dritten Rechtsbereinigungsgesetzes	Schriftliche Stellungnahmen gegenüber Ausschüssen des Deutschen Bundestages sowie gegenüber dem BMA und dem BMV
Entwurf eines Gesetzes zur Umsetzung der Richtlinie des Rates über die Umweltverträglichkeitsprüfung	Schriftliche und mündliche Stellungnahmen gegenüber Ausschüssen des Deutschen Bundestages und dem BMU
Poststrukturgesetz	— Beratungen mit BMP, BMJ und BMWi — Schriftliche und mündliche Stellungnahmen gegenüber den zuständigen Ausschüssen des Deutschen Bundestages
Gesetz zur Einführung des Sozialversicherungsausweises	Beratung und schriftliche Stellungnahme gegenüber dem Ausschuß für Arbeit und Sozialordnung, dem Innenausschuß des Deutschen Bundestages und dem BMA
Datei ADOS	Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI, Informationsbesuch beim BfV
Entwurf eines Katastrophenschutzergänzungsgesetzes	Schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI
Rentenreformgesetz 1992 (RRG 1992)	Beratung und schriftliche Stellungnahme gegenüber dem Ausschuß für Arbeit und Sozialordnung des Deutschen Bundestages und dem BMA
Entwurf eines Gesetzes zur Verbesserung der Überwachung des Außenwirtschaftsverkehrs und Entwurf eines Sechsten Gesetzes zur Änderung des Außenwirtschaftsgesetzes	Schriftliche Stellungnahme gegenüber dem Wirtschaftsausschuß des Deutschen Bundestages und dem BMWi
Gesetz über die Errichtung eines Bundesamtes für Strahlenschutz	Beratung und schriftliche Stellungnahme gegenüber dem Ausschuß für Umwelt, Naturschutz und Reaktorsicherheit des Deutschen Bundestages und dem BMU

Thema	Art der Erledigung
Entwurf eines Gesetzes zur Ergänzung des Katastrophenschutzgesetzes und anderer Vorschriften	Beratung und schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI
Entwurf einer Gemeinschaftscharta der Sozialen Grundrechte	Schriftliche Stellungnahme gegenüber dem Bundesrat
Gefahrgutbeauftragtenverordnung	Beratung und schriftliche Stellungnahme gegenüber dem Bundesrat und dem BMV
Gefahrgutänderungsverordnung Straße	Beratung und schriftliche Stellungnahme gegenüber dem Bundesrat und dem BMV
Entwurf eines Gesetzes über den Auswärtigen Dienst	Schriftliche Stellungnahme gegenüber dem AA
Entwurf eines Gesetzes über das Ausländerzentralregister sowie Entwurf einer Verordnung zur Durchführung dieses Gesetzes	Beratung und schriftliche Empfehlungen gegenüber dem BMI
Zusatzübereinkommen zum Übereinkommen von Schengen	Beratung und schriftliche Stellungnahme gegenüber dem BMI; Mitwirkung am Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie an der Erklärung der Datenschutzkontrollinstitutionen von Frankreich, Luxemburg und der Bundesrepublik Deutschland
Prüfung der Rechtmäßigkeit von ZEVIS-Abfragen durch das Bundeskriminalamt anhand der Protokollauswertungen durch das Kraftfahrt-Bundesamt	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Entwicklung der Datenverarbeitung beim Bundeskriminalamt	Schriftliche Stellungnahme gegenüber dem BMI
Neufassung des Meldedienstes in Rauschgiftsachen	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Auswirkungen meiner Prüfung bei der Abteilung Staatsschutz auf die Datenverarbeitung in APIS	Beratung, Erörterungen mit BMI und BKA
Verkartungspläne verschiedener Abteilungen des BfV	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Durchführung des Gesetzes über Personalausweise und des Paßgesetzes	Schriftliche Empfehlungen an den BMI
Entwurf einer Verordnung über die Benutzung des Bundesarchivs	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Entwurf eines Gesetzes zur Regelung der Rechtsverhältnisse der Helfer der Bundesanstalt THW und Verordnungen hierzu	Schriftliche Stellungnahme gegenüber dem BMI
Entwurf für ein Gesetz zur Neuregelung des Ausländerrechts	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMI

Thema	Art der Erledigung
Strafverfahrensänderungsgesetz	Beratung und schriftliche Empfehlungen gegenüber BMJ
Zivilprozeßordnung	Schriftliche Empfehlungen zu verschiedenen Problembereichen gegenüber dem BMJ
Arbeitsentwurf eines Dritten Gesetzes zur Änderung des Bundeszentralregistergesetzes	Beratung und schriftliche Stellungnahmen gegenüber dem BMJ
Entwurf eines Betreuungsgesetzes	Schriftliche Stellungnahme gegenüber dem BMJ
Regierungsentwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis und Entwurf einer Verordnung über die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis	Schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Gesetzes bereichsspezifischer Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung	Schriftliche Stellungnahme gegenüber dem BMF
Entwurf einer Kontrollmitteilungsverordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMF
Entwurf einer Steuerdaten-Abruf-Verordnung	Beratung gegenüber dem BMF
Verfahren der zollrechtlichen Überwachung	Erörterung mit dem BMF
Versicherungsaufsichtsgesetz	Schriftliche Stellungnahme gegegenüber dem BMF
Anpassung des Gewerbeverwaltungsrechts an die datenschutzrechtlichen Vorgaben des Bundesverfassungsgerichts	Schriftliche Stellungnahme gegenüber dem BMWi
Förderung der Unternehmensberatung	Beratung und schriftliche Stellungnahme gegenüber dem BMWi und dem Bundesamt für Wirtschaft
Entwurf eines Ernährungsvorsorgesetzes und Entwurf eines Ernährungssicherstellungsgesetzes	Schriftliche Stellungnahme gegenüber dem BML
Berufskrankheitenverordnung	Beratung des BMA
Vorschlag der Kommission der Europäischen Gemeinschaften für die Verordnung (EWG) des Rates zur Änderung der Verordnungen (EWG) Nr. 1408/71 und Nr. 574/72 (Kindergeld nach überstaatlichem Recht; Datenabgleich)	Beratung und schriftliche Stellungnahme gegenüber dem BMA und der Bundesanstalt für Arbeit
Gesetz zur Förderung der Einstellung der Landwirtschaftlichen Erwerbstätigkeit (FELEG)	Beratung und schriftliche Stellungnahme gegenüber dem BMA
KLIMACS (Klinisch-medizinische Analysen — Computer System — Programm, das die klinische Dokumentation der Daten von AIDS-Patienten unterstützt)	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Neufassung der Sicherheitsrichtlinien für den Bereich des BMVg (Zentrale Dienstvorschrift)	Beratung und schriftliche Stellungnahme gegenüber dem BMVg

Thema	Art der Erledigung
KLINAIDS (Multizentrische Studie zum klinischen Verlauf der HIV-Infektion)	Beratung und schriftliche Stellungnahme gegenüber dem BMJFFG und dem BGA
Änderung des Bundeskindergeldgesetzes (BKGG)	Schriftliche Stellungnahme gegenüber dem BMJFFG
Kinder- und Jugendhilfegesetz (KJHG)	Schriftliche Stellungnahme gegenüber dem BMJFFG
Entwurf eines Ersten Gesetzes zur Änderung des Heimgesetzes	Beratung des BMJFFG
Gentechnikgesetz	Schriftliche Stellungnahme gegenüber dem BMJFFG
Entwurf eines Gesetzes zur Änderung des Chemikaliengesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMU
Verbrauchsdatenerfassung mit TEMEX	Beratungen von BMPT, BMJ und BMWi
Zugangssicherung zum DATEX-P-Dienst	Schriftliche Stellungnahme gegenüber dem BMPT
Cityruf-Dienst der DBP	Beratung des BMPT
Verbindungsdatenspeicherung bei Telekommunikationsdiensten	Beratungen und schriftliche Stellungnahmen gegenüber dem BMPT
Änderung der Postordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMPT
Änderung der Postgiroordnung	Beratung und schriftliche Stellungnahme gegenüber dem BMPT
Btx-Kontonummernauskunft im Postgirodienst	Schriftliche Empfehlung gegenüber BMPT
Gesetz zum Abbau der Fehlsubventionierung im Wohnungsbau	Schriftliche Stellungnahme gegenüber dem BMBau
Einführung der automatisierten Fahrkartenausgabe bei der Deutschen Bundesbahn	Beratung der Deutschen Bundesbahn
Schülerbeförderung; Abrechnungsverfahren zwischen den Landkreisen und der Deutschen Bundesbahn	Unterbreitung eines Vorschlages zur Änderung des Verfahrens gegenüber der Deutschen Bundesbahn
Schwarzfahrerkartei	Kontrolle und Beratung des Geschäftsbereichs Bahnbus Rheinland
Wahrnehmung von Aufgaben der Betriebskrankenkasse durch die Dienststellen des BMV	Beratung der Betriebskrankenkasse des BMV
Europäischer und Internationaler Datenschutz	Durchführung der 11. Internationalen Konferenz der Datenschutzbeauftragten im August 1989, Entschließungen u. a. über grenzüberschreitenden Datenverkehr
Krebsregister	Mündliche und schriftliche Stellungnahme im Rahmen der 4. Großen Krebskonferenz am 5. Dezember 1989 in Bonn

Thema	**Art der Erledigung**
Einsatz von Arbeitsplatzcomputern	Beratungen und schriftliche Stellungnahmen und Übersendung einer Arbeitshilfe an die obersten Bundesbehörden
Automatisierte Personaldatenverarbeitung einschließlich APC-Einsatz, Beihilfe-, Telefondaten- und Textverarbeitung sowie entsprechende Dienstvereinbarungen	Beratungen und schriftliche Stellungnahmen gegenüber mehreren Behörden und Personalvertretungen
Wartung und Fernwartung von Telefonnebenstellenanlagen	Informationsgespräche und Beratungen mit Herstellern

1.3 Beanstandungen

Die förmliche „Beanstandung" nach § 20 Abs. 1 des Bundesdatenschutzgesetzes ist meine „schärfste Waffe" gegenüber der Verwaltung. Mehr als beanstanden kann ich ihr gegenüber nicht; das Bundesdatenschutzgesetz sieht insbesondere keine Möglichkeit vor, Beanstandungen gegenüber der Verwaltung auch durchzusetzen. Die einzige Möglichkeit, eine Behörde, die sich weigert, einer Beanstandung zu entsprechen — was auch im Berichtsjahr vorgekommen ist — doch noch zum Einlenken zu bewegen, besteht darin, daß ich mich nach § 19 Abs. 2 Satz 4 BDSG an den Deutschen Bundestag wende. Von dieser Möglichkeit mache ich außerhalb des Tätigkeitsberichts naturgemäß nur in Fällen von politischer Bedeutung Gebrauch. Wenn ich feststelle, daß eine Behörde oder öffentliche Stelle des Bundes gegen das Bundesdatenschutzgesetz oder gegen andere Datenschutzbestimmungen verstoßen hat oder wenn sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, so habe ich dies nach § 20 BDSG zu beanstanden; lediglich bei unerheblichen Mängeln kann ich darauf verzichten (§ 20 Abs. 2 BDSG). Als unerhebliche Mängel bewerte ich insbesondere Verstöße im Einzelfall, bei denen die Behörde den Rechtsverstoß oder Mangel einräumt und umgehend abstellt. Voraussetzung ist ferner, daß noch keine schwerwiegenden Nachteile für den Betroffenen entstanden sind oder bereits entstandene Schäden umgehend beseitigt werden.

Habe ich eine Beanstandung nach § 20 Abs. 1 BDSG ausgesprochen, kann allein aus der Tatsache der Beanstandung nicht stets auf die Schwere des Rechtsverstosses geschlossen werden; dazu bedarf es der Kenntnis des konkreten vollständigen Sachverhaltes. Die Zahl der im Berichtsjahr ausgesprochenen förmlichen Beanstandungen liegt ziemlich genau auf der Höhe der beiden letzten Jahre. Einzelheiten zu den Beanstandungen ergeben sich aus den jeweiligen Berichtsteilen, auf die jeweils verwiesen wird.

Beanstandungen wurden im Berichtsjahr ausgesprochen gegenüber:

Bundesminister des Innern	Rechtswidrige automatisierte Abrufe von Fahrerlaubnisdaten aus dem Verkehrszentralregister und von Daten aus dem Zentralen Fahrzeugregister beim Kraftfahrt-Bundesamt (siehe 8.1.2)
Bundesminister der Finanzen	— Unzulässige Datenübermittlung durch das Zollkriminalinstitut an eine Polizeidienststelle; Verstoß gegen § 30 AO (siehe 18.1) — Gewährung des online-Zugriffs durch die Berliner Polizei auf den Datenbestand „Zollrechtliche Überwachung"; Verstoß gegen § 10 BDSG (siehe 18.2)
Bundesminister der Verteidigung	Mangelnde Erforderlichkeit der Speicherung personenbezogener Daten zur rechtmäßigen Erfüllung der Aufgaben des Streitkräfteamtes (Verstoß gegen § 9 Abs. 1 BDSG), Unterlassung der Veröffentlichung (Verstoß gegen § 12 BDSG), langjährige Nichtaufnahme von Dateien in die Dateienübersicht (Verstoß gegen § 15 BDSG), (siehe 20.1)

Bundesminister für Verkehr	Verstoß des Kraftfahrt-Bundesamtes gegen § 30a StVG durch Gewährung eines unzulässigen automatisierten Abrufs von Fahrerlaubnisdaten an das Bundeskriminalamt (siehe 8.1.2)
Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit	Nicht ordnungsgemäßer Einsatz von Arbeitsplatzcomputern in verschiedenen Arbeitseinheiten im Ministerium; Verstoß gegen §§ 6 und 15 BDSG (siehe 24.2.2)
Bundesminister für Post und Telekommunikation	— Unzulässige Speicherung der Verbindungsdaten bei ISDN; Verstoß gegen § 9 BDSG (siehe 7.2.3) — Zweckwidrige Verwertung einer Bundeszentralregisterauskunft aus der Sicherheitsüberprüfung in einem Einzelfall (§ 41 Abs. 4 BZRG); (siehe 19.1) — Unzureichende Sicherstellung des internen Datenschutzes bei einem Postgiroamt; Verstoß gegen § 15 BDSG (siehe 7.8)
Bundesanstalt für Arbeit	Verstoß gegen § 35 SGB I (Sozialgeheimnis) durch zwei Arbeitsämter in Einzelfällen sowie gegen § 84 SGB X (unzulässige Datenspeicherung) durch zwei weitere Arbeitsämter in Einzelfällen (siehe 12.1 und 12.4)
Vorstand der Deutschen Bundesbahn	Speicherung von Schwarzfahrten strafunmündiger Kinder; Verstoß gegen § 9 BDSG (siehe 8.6.1)
Bau-Berufsgenossenschaft Wuppertal	Nicht ordnungsgemäße Entsorgung von EDV-Listen/ unbefugte Offenbarung; Verstoß gegen § 35 SGB I (siehe 15)
Versorgungsanstalt der Deutschen Bundespost	Unbefugte Offenbarung und fehlende Maßnahmen zur Wahrung des Personaldatenschutzes und des Schutzes von Gesundheitsdaten; Verstöße gegen § 35 SGB I und Nr. 10 der Anlage zu § 6 BDSG (siehe 11.3)

Von diesen Maßnahmen messe ich den Beanstandungen

- gegenüber dem BMF betreffend die Gewährung des online-Zugriffs durch die Berliner Polizei auf den Datenbestand „Zollrechtliche Überwachung" und

- gegenüber dem BMPT wegen unzulässiger Speicherung der Verbindungsdaten bei ISDN

besondere Bedeutung zu, weil die beanstandeten Maßnahmen zu Hunderttausenden unzulässigen Datenverarbeitungen führen können. Die zuständigen Stellen haben in diesen Fällen auch noch keine Konsequenzen aus meinen Beanstandungen gezogen.

Besonders hinzuweisen ist auch auf die Beanstandungen

- gegenüber dem Bundesminister des Innern und dem Bundesminister für Verkehr wegen jahrelanger unzulässiger automatisierter Abrufe von Fahrerlaubnisdaten aus dem Verkehrszentralregister durch das Bundeskriminalamt

- gegenüber dem BMVg wegen nicht erforderlicher Datenspeicherungen für Aufgaben der psychologischen Verteidigung beim Streitkräfteamt und

- gegenüber der Deutschen Bundesbahn wegen der Speicherung von Daten strafunmündiger Kinder, die als Schwarzfahrer festgestellt worden waren, über den Zeitpunkt der Zahlung des erhöhten Beförderungsgeldes hinaus.

Die beiden letzteren Vorgänge haben in den Medien besondere Beachtung gefunden. Die Deutsche Bundesbahn setzt trotz meiner Beanstandung die Speicherung strafunmündiger Kinder auch nach Zahlung des erhöhten Beförderungsentgelts fort. Dagegen wurden die unzulässigen Abrufe aus dem Verkehrszentralregister im Zusammenhang mit der von mir durchgeführten Kontrolle unverzüglich eingestellt. Auch der Bundesminister der Verteidigung hat die beanstandete Datenspeicherung beim Streitkräfteamt aufgegeben und die angelegten Dateien vernichtet.

1.4 Zusammenarbeit mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz sowie mit anderen Stellen

Auch im Berichtsjahr wurden datenschutzrechtlich wichtige Themen zusammen mit den Landesbeauftragten für den Datenschutz und der Datenschutzkommission Rheinland-Pfalz in Entschließungen der Konferenz behandelt und in deren Arbeitskreisen diskutiert. Auf den drei Konferenzen der Datenschutzbeauftragten des Bundes und der Länder, deren Vorsitz im Berichtsjahr das Saarland hatte, wurden Entschließungen zu folgenden Themen gefaßt:

- Neuregelung des Bundesdatenschutzgesetzes (Entschließung vom 5./6. April 1989, Anlage 1)
- Änderung des Gesetzes zu Artikel 10 GG und der Strafprozeßordnung im Rahmen der Poststrukturreform (Entschließung vom 5./6. April 1989, Anlage 2)
- Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Entschließung vom 5./6. April 1989, Anlage 3)
- Entwurf eines Rentenreformgesetzes 1992 (Entschließung vom 5./6. April 1989, Anlage 4)
- Entwürfe eines Bundesverfassungsschutzgesetzes (BVerfSchG), eines MAD-Gesetzes (MADG) und eines BND-Gesetzes (BNDG) (Entschließung vom 30. Mai 1989, Anlage 5)
- Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen (Entschließung vom 26./27. Oktober 1989, Anlage 6)
- Genomanalyse und informationelle Selbstbestimmung (Entschließung vom 26./27. Oktober 1989, Anlage 7)
- Datenschutz in der Europäischen Gemeinschaft (Entschließung vom 26./27. Oktober 1989, Anlage 8)
- Entwurf einer EG-Statistikverordnung (Entschließung vom 26./27. Oktober 1989, Anlage 9)

Mit der Nationalen Kommission für die Informatik und die Freiheiten (CNIL) der Französischen Republik und der beratenden Kommission nach dem Datenschutzgesetz des Großherzogtums Luxemburg habe ich am 16. März 1989 eine Erklärung zum Datenschutz bei dem von den Unterzeichnerstaaten des Schengener Übereinkommens geplanten gemeinsamen Informationssystem erarbeitet (s. Anlage 12). Überhaupt hat sich im Berichtsjahr stärker als bisher gezeigt, daß mit dem Zusammenwachsen der europäischen Staaten auch eine stärkere Kooperation mit ausländischen Datenschutzinstitutionen erforderlich ist (s. hierzu insbesondere den Abschnitt 27 dieses Berichts).

Nach wie vor zeigte sich als wichtig, daß ich mich als Teilnehmer an den Sitzungen und durch Mitarbeit in besonderen Arbeitsgremien des Düsseldorfer Kreises, in dem die Aufsichtsbehörden der Länder ihre gemeinsamen Probleme beraten, über den Datenschutz im nicht-öffentlichen Bereich informieren kann. Insbesondere in den Fällen, in denen der Bundesgesetzgeber oder Bundesbehörden aufgrund ihrer Zuständigkeiten Einfluß auf die Datenverarbeitung der Wirtschaft nehmen, zeigt sich, wie wichtig es ist, daß ich im Düsseldorfer Kreis als Bindeglied zwischen den jeweiligen Institutionen des Bundes und dem nicht-öffentlichen Bereich wirken kann (s. nachfolgend Abschnitte 21 und 26).

Mehrfach habe ich die Gelegenheit wahrgenommen, mit den Vertretern von Firmen, die DV-Anlagen herstellen, über zukünftige technische und ökonomische Entwicklungen und die daraus zu erwartende Folgen für den Datenschutz zu diskutieren. Ich beabsichtige, diese Gespräche ebenso fortzusetzen wie die mit Vertretern von Wirtschaftszweigen, in denen in großem Umfang personenbezogene Daten verarbeitet werden und in denen deshalb dem Datenschutz eine erhebliche Bedeutung zukommt.

Vertreter meiner Dienststelle haben auch im Berichtsjahr regelmäßig oder bei Bedarf an Sitzungen des interministeriellen Ausschusses für die Sicherheit in der Informationstechnik (ISIT), der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) und von Gremien des Deutschen Instituts für Normung e. V. (DIN) teilgenommen.

1.5 Öffentlichkeitsarbeit

Wie auch in den Vorjahren ist das Interesse der Öffentlichkeit an meiner Arbeit groß. Auch im Berichtsjahr hat meine Dienststelle über fünfzig Besuchergruppen betreut. Ein stärkeres Engagement in diesem interessanten Aufgabenfeld ist aufgrund der Personalstärke der Dienststelle nicht möglich. Ich freue mich jedoch darüber, daß mir von den Büros mehrerer Mitglieder des Deutschen Bundestages versichert wurde, sie legten Wert darauf, regelmäßig Besuchergruppen schicken zu können, da die Gruppen den Besuch und die Information in meinem Hause häufig als „besonders interessant" bezeichnen. Diese positive Annahme ist für meine Mitarbeiter und mich sehr wichtig, da gerade über die Besuchergruppen eine Öffentlichkeit erreicht wird, an die mit den mir sonst zur Verfügung stehenden Mitteln Informationen über den Datenschutz nur sehr schwer herangetragen werden können. Zugleich erhalte ich aus den oft sehr offenen Gesprächen wertvolle Anregungen für meine Arbeit.

Nach wie vor groß ist das Interesse an den von mir herausgegebenen Broschüren

- Bürgerfibel Datenschutz
- Der Bürger und seine Daten.

Die Broschüre „Der Bürger und seine Daten im Netz der sozialen Sicherung" wird nach wie vor oft erbeten. Leider konnte ich sie im Laufe des Berichtsjahres noch nicht an die neueste Entwicklung (insbesondere Berücksichtigung des Gesundheits-Reformgesetzes und des Rentenreformgesetzes) anpassen. Ich hoffe, daß mir dies 1990 gelingt und damit eine — wie die Erfahrung zeigt — wichtige Information den Bürgern wieder zur Verfügung gestellt werden kann. Aufgrund

von Einzelanforderungen, aber auch von Sammelbestellungen für Unterrichts- und Schulungszwecke von Bildungseinrichtungen, Behörden und Firmen, habe ich im Berichtsjahr rund 78 000 Broschüren versandt.

Überwiegend aus aktuellem Anlaß haben meine Mitarbeiter und ich zahlreiche Presse-, Rundfunk- und Fernsehinterviews gegeben und Journalisten über Fragen des Datenschutzes und die damit zusammenhängende Datenverarbeitung informiert. Mein Eindruck bleibt bestätigt, daß meine Dienststelle von vielen Journalisten als hilfreich empfunden wird, wenn zum Verständnis von politischen Ereignissen Hintergrundwissen uber die Datenverarbeitung in der Verwaltung erforderlich ist. In wenigen Fällen bin ich wieder von mir aus mit Erklärungen an die Öffentlichkeit getreten. In diesem Zusammenhang wird mir gelegentlich vorgehalten, daß ich von dieser Möglichkeit, aktiv die Öffentlichkeit zu informieren, zu selten Gebrauch mache. Ich stelle jedoch häufig fest — und dies zeigen insbesondere die Hintergrundgespräche mit Journalisten —, daß sich nicht alle Vorgänge im Bereich des Datenschutzes medienwirksam aufbereiten lassen. Auch gilt es für mich immer abzuwägen, was wichtiger ist: die Öffentlichkeit zu informieren oder in intensiven Gesprächen mit einer Behörde für die Bürger ein gutes Ergebnis zu erreichen, was häufig leichter und rascher möglich ist, wenn eine gewisse Diskretion gewahrt werden kann.

Zugenommen hat im Berichtsjahr die Nachfrage nach Referenten aus meiner Dienststelle für Vorträge und Seminarveranstaltungen, bei denen ich häufig auch persönlich als Vortragender auftrete. Insbesondere bei den Seminaren zeigte sich, daß der Wunsch, mehr darüber zu erfahren, wie man mit Computern sicher arbeiten kann, deutlich häufiger als früher geäußert wird. Es ist erfreulich, daß die Bundesakademie für öffentliche Verwaltung sich gerade um die Veranstaltung solcher Seminare bemüht und sogar bereit ist, entsprechende Sonderseminare zu organisieren.

Der Bundesminister des Innern hat im Berichtsjahr wieder Ergebnisse einer Untersuchung über Einstellungen zu aktuellen Fragen der Innenpolitik vorgelegt, die vom Mannheimer Institut für praxisorientierte Sozialforschung (ipos) Ende April/Anfang Mai 1989 durchgeführt wurde. Die Ergebnisse dieser Untersuchung sind repräsentativ für die wahlberechtigte Bevölkerung in der Bundesrepublik Deutschland. Mit dieser Untersuchung wurde wieder bestätigt, daß der Bundesbeauftragte für den Datenschutz als eine sehr wichtige Einrichtung angesehen wird. Dabei lag meine Behörde unter den zehn vorgegebenen Institutionen aus dem Geschäftsbereich des Bundesminister des Innern an der dritten Stelle, was angesichts der geringen Größe der Dienststelle ein sehr gutes Ergebnis ist.

1.6 Die Dienststelle

Durch die Bewilligung von je einer Planstelle des höheren und des gehobenen Dienstes im Haushaltsplan 1990 hat sich die Personalsituation meiner Dienststelle verbessert. Es ist nunmehr der bei der Errichtung der Dienststelle im Jahre 1977 geplante Personalstand erreicht. Zwischenzeitlich hat es jedoch eine solche Vielzahl von Entwicklungen gegeben, daß eine weitere personelle Verstärkung notwendig ist. Wie ich bereits in meinem 11. Tätigkeitsbericht ausgeführt habe, war die Einrichtung eines selbständigen Referats „Informationstechnik“ unumgänglich. Der durch den rasch zunehmenden Einsatz von Arbeitsplatz-Computern, Systemvernetzungen und den Neuen Medien gekennzeichnete Entwicklungsstand der Datenverarbeitungstechnik hat einen enormen Beratungs- und Kontrollbedarf zur Folge; die Bundesbehörden, einschließlich der bundesunmittelbaren Körperschaften im Bereich der Sozialverwaltung, erwarten — sensibilisiert durch Hackererfolge — zu Recht mehr als bisher fachkundige Beratung durch den BfD auf dem Gebiet der Datensicherheit. Dazu bin ich gesetzlich verpflichtet.

Gesundheits- und Rentenreform wie auch äußerst schwierige datenschutzrechtliche Probleme im Zusammenhang mit Fragen der inneren Sicherheit, des Ausländer- und Asylrechts, des Ausländerzentralregisters, des Extremismus, Terrorismus und der Spionageabwehr, um nur einige Beispiele zu nennen, verlangen immer mehr Beratung und Kontrolle.

Auch der ständige Aufgabenzuwachs im internationalen Rahmen ist offenkundig. Der Ausbau der Europäischen Gemeinschaft und die zunehmende internationale Verflechtung rücken Fragen des Datenschutzes immer mehr in den Mittelpunkt der Betrachtung und bedingen insbesondere im Hinblick auf eine koordinierte Entwicklung großen Arbeitsaufwand.

Die Darstellung der Kontrollen und Beratungen unter Nr. 1.2 zeigt deutlich, in welchem Ausmaß meine Dienststelle durch die Beratungsaufgabe allein im Bereich der Gesetzgebung gefordert wird. Bei der Beteiligung an umfangreichen Gesetzgebungswerken (etwa Rentenreform, Strafverfahrensänderungsgesetz, Ausländergesetz) ist für die Durchdringung der Entwürfe und ihre Bewertung unter Datenschutzaspekten eine sehr zeitraubende Mitprüfung erforderlich. Die dafür aufzuwendende Arbeitskraft, deren Einsatz unbedingt notwendig ist, reduziert naturgemäß die Möglichkeit für Kontrollen. Angesichts des zunehmenden Einsatzes von Datenverarbeitungstechnik, der erfahrungsgemäß besondere Risiken mit sich bringt, ist aber nicht eine Reduzierung, sondern eine Erhöhung der Kontrolldichte erforderlich.

Vor diesem Hintergrund werde ich für den Haushalt 1991 meinen dringlichsten Stellenbedarf darstellen und gleichzeitig entsprechend meinem Personalbedarf im Rahmen des Finanzplanungszeitraums anmelden.

Ich hoffe, daß ich die notwendige Unterstützung finde.

2 Deutscher Bundestag — PARLAKOM —

Am 27. Februar 1986 beschloß der Ältestenrat des Deutschen Bundestages, „zur Verbesserung der Arbeitsmöglichkeiten und Arbeitsbedingungen seiner

Mitglieder und der Mitarbeiterinnen und Mitarbeiter ein gemeinsames Informations- und Kommunikationssystem für das Parlament, die Fraktionen und die Wahlkreisbüros der Abgeordneten" einzuführen. Er erkannte dabei die Notwendigkeit, „den Problemen von Datenschutz und Datensicherheit Rechnung zu tragen" und verlangte bereits vor Beginn des vorgesehenen Modellversuchs die Einrichtung eines unabhängigen Datenschutzgremiums, in dem neben Vertretern der Fraktionen auch die Verwaltung des Deutschen Bundestages mitwirken sollte. Seitdem wurden für PARLAKOM rund 60 Mio. DM ausgegeben und die Büros von etwa 240 Abgeordneten mit Arbeitsplatzcomputern ausgerüstet sowie die sonstigen Voraussetzungen geschaffen. Dabei handelt es sich grundsätzlich um Einzelplatzsysteme, von denen jeweils zwei im Bonner Büro und eines im Wahlkreisbüro des Abgeordneten eingerichtet sind. Bis zu einem echten parlamentarischen Informations*system* ist noch ein weiter Weg: Ein schneller Informationsaustausch — etwa eine Abfrage des Gesetzgebungs-Informationssystems GESTA vom Wahlkreisbüro aus — ist noch nicht möglich und nur wenige Abgeordnete haben die Möglichkeit, über das Netz der Deutschen Bundespost Recherchen in externen Datenbanken durchzuführen, wie z. B. in denen der Europäischen Gemeinschaft.

In einer vom Ältestenrat erbetenen Stellungnahme hatte ich die Notwendigkeit eines integrierten Datenschutzkonzeptes betont, das von den rechtlichen und organisatorischen Besonderheiten der drei Anwendungsbereiche — Abgeordneter, Fraktion, Verwaltung — ausgeht und unter Berücksichtigung der Grundsätze von Datenschutz und Datensicherheit Empfehlungen und Regelungen zum Schutz personenbezogener Daten enthält. Ich habe betont, daß es dabei auch darauf ankommt, Prinzipien für die *Zulässigkeit* der Verarbeitung personenbezogener Daten zu entwickeln (vgl. 9. TB S. 13 f.; 10. TB S. 14).

Dem auf Empfehlungen des Ältestenrates eingerichteten Datenschutzgremium liegen inzwischen von der Verwaltung überarbeitete Entwürfe eines „Integrierten Datenschutz- und Datensicherungskonzeptes für den Deutschen Bundestag" (Datenschutzkonzept) und von „Empfehlungen an die Mitglieder des Deutschen Bundestages für den Einsatz von Informations- und Kommunikationstechniken" vor.

Insbesondere das „Datenschutzkonzept" gibt wichtige und praxisorientierte Hinweise, die nach meiner Überzeugung gut geeignet sind, die in PARLAKOM verarbeiteten personenbezogenen Daten gegen unberechtigte Benutzung zu schützen und ihre Verfügbarkeit zu erhalten. Ich habe es begrüßt, daß auch den Abgeordneten und Fraktionen das Führen von Bestandsverzeichnissen — sowohl über die Art der gespeicherten personenbezogenen Daten als auch über die Hard- und Software — empfohlen wird, wie sie die Vorschriften des § 15 BDSG von den Behörden der Bundesverwaltung verlangen. Das „Datenschutzkonzept" berücksichtigt bisher nicht ausreichend die rechtliche und organisatorische Unterschiedlichkeit der drei Anwendergruppen und geht nicht auf die Datenflüsse zwischen diesen Gruppen untereinander — z. B. zwischen Abgeordneten und Ausschuß — sowie zwischen ihnen und anderen Stellen ein. Entscheidender Schwachpunkt ist, daß materielle Fragen des Datenschutzes — etwa nach der Zulässigkeit der Datenverarbeitung — bisher noch keine Berücksichtigung gefunden haben. Ich hatte der Verwaltung des Deutschen Bundestages zunächst empfohlen, den Entwurf insoweit zu ergänzen. Bei den weiteren Erörterungen wurde allerdings darauf hingewiesen, daß weder das geltende BDSG noch der Regierungsentwurf zu seiner Novellierung auf die besonderen Fragen eingehen, die bei der Verarbeitung personenbezogener Daten durch den Deutschen Bundestag und seine Mitglieder auftreten, z. B. in bezug auf die Kontrolle der Datenverarbeitung. Die Kommission des Ältestenrates des Deutschen Bundestages für den Einsatz neuer Informations- und Kommunikationstechniken und -medien hat deshalb den Ältestenrat aufgefordert, sich im Rahmen der Novellierung des BDSG um eine sachgerechte Lösung zu bemühen. Es bleibt abzuwarten, welches Ergebnis diese Anregung haben wird. Davon wird auch abhängen, welchen Inhalt die notwendigen Erläuterungen und Hinweise zur Zulässigkeit der Verarbeitung personenbezogener Daten und zu den Pflichten der speichernden Stellen im Rahmen von PARLAKOM haben werden.

Im übrigen teile ich auch die Auffassung der Verwaltung des Deutschen Bundestages, die in den oben genannten Entwürfen zum Ausdruck kommt, daß der Sicherung der in PARLAKOM verarbeiteten personenbezogenen Daten wegen der möglichen Folgen bei einer mißbräuchlichen Einsichtnahme oder Verwendung besondere Bedeutung beizumessen ist.

Um mir einen Eindruck vom erreichten Sicherheitsniveau zu verschaffen, kontrollierte ich im September 1989 die von der Verwaltung gemäß § 6 BDSG getroffenen organisatorischen und technischen Maßnahmen zur Sicherstellung des Datenschutzes bei PARLAKOM. Dabei beschränkte sich die Kontrolle auf solche Geräte und Verfahren, die nur von der Verwaltung für eigene Zwecke eingesetzt waren. Mir wurde erklärt, dies treffe auf die etwa 90 Geräte im Schulungszentrum und im Benutzer-Servicezentrum zu, die zur Aus- und Weiterbildung sowie zur weiteren Betreuung der Anwender im parlamentarischen Bereich betrieben werden. Nach Angaben der Verwaltung werden in diesem Zusammenhang ausschließlich „Übungsdateien" benutzt; personenbezogene Daten existierender natürlicher Personen werden weder gespeichert noch verarbeitet.

Von der Datenschutzkontrolle ausgenommen waren sowohl die von den Abgeordneten selbst benutzten Geräte als auch die etwa 30 im organisatorischen Umfeld der parlamentarischen Arbeit eingesetzten Geräte, d. h. im Bereich der Vizepräsidenten und in den Sekretariaten von sieben Ausschüssen des Deutschen Bundestages.

Wie oben dargelegt, handelt es sich bei den PARLAKOM-Geräten um Einzelplatzrechner; die Hardware kann aus einer Liste von derzeit sieben verschiedenen Herstellern ausgesucht werden. Die vorhandene Software erlaubt die Anwendungen

- Textverarbeitung,
- Ablageverwaltung,
- Adreßverwaltung,
- Terminkalender,
- Teletex,
- Zugang zu eigenen Datenbanken des Deutschen Bundestages sowie
- für die Abgeordneten, die bereits am Modellversuch teilgenommen haben: Zugang zu öffentlichen Datenbanken sowie zu anderen über das Datennetz der DBP erreichbaren Rechnern.

Ich habe den Eindruck gewonnen, daß sowohl die Grundeinweisung und die Fortbildung als auch die Unterstützung der Anwender nach einem sorgfältig durchdachten, überzeugenden Konzept erfolgen. Positiv hervorzuheben ist, daß bereits im Rahmen eines Basiskursus auf Probleme der Datensicherung sowie Lösungsmöglichkeiten hingewiesen wird. Es erscheint jedoch unerläßlich, auch auf Aspekte der Erforderlichkeit der Datenverarbeitung einzugehen und die entsprechende Unterrichtseinheit insoweit zu erweitern. Für die bereits geschulten Anwender kommt die Einrichtung entsprechender Workshops in Frage. Begrüßt habe ich, daß eine Reihe von Datensicherungsforderungen bei den PARLAKOM-Geräten schon Berücksichtigung gefunden haben. So besteht die Möglichkeit, durch Festlegen eines Paßwortes die Adreßverwaltung und die Kommunikationsanwendungen zu schützen. Auch wurde mir mitgeteilt, daß die Adreßdateien verschlüsselt abgespeichert werden. Dadurch sind dem Anwender mit „normaler" Ausbildung Zugriffe auf die entsprechenden Anwendungen nur in dem Umfange eröffnet, wie sie ihm der Befugte — z. B. der Abgeordnete — gestattet hat. Einem Anwender mit weitergehenden Kenntnissen ist es jedoch grundsätzlich möglich, sich Zugang zum Betriebssystem zu verschaffen und dann die genannten Schutzmechanismen zu umgehen. Ich habe daher der Verwaltung des Deutschen Bundestages empfohlen, zumindest bei der Verarbeitung sensiblerer personenbezogener Daten zusätzliche Maßnahmen zum Schutz gegen unbefugten Zugriff zu treffen. Solche „Sicherheitspakete" werden auf dem Markt von mehreren Herstellern angeboten (s. hierzu 24.2.4 sowie 11. TB S. 84 f.). Damit kann auch ein generelles, hier besonders wichtiges Problem der elektronischen Datenverarbeitung gelöst werden: „Gelöschte" Daten (Briefe usw.) bleiben in der Regel im Speicher (Platte, Diskette) erhalten und grundsätzlich lesbar; lediglich der Dateiname wird im „Inhaltsverzeichnis" gelöscht und damit das Auffinden erschwert. Einige Sicherheitspakete ermöglichen demgegenüber ein wirkliches (physikalisches) Löschen und erhöhen auch hierdurch die Sicherheit.

Insgesamt habe ich den Eindruck gewonnen, daß die Verwaltung des Deutschen Bundestages in verstärktem Maße den Problemen des Datenschutzes und der Datensicherheit Aufmerksamkeit zugewandt hat. Dies kommt u. a. in den erarbeiteten Entwürfen einer neuen „Dienstanweisung Datenschutz" und einer „Dienstanweisung zur Überwachung der Einhaltung datenschutzrechtlicher Vorschriften" zum Ausdruck. Ich gehe davon aus, daß diese Entwürfe demnächst in Kraft gesetzt werden.

3 Innere Verwaltung

3.1 Melderecht

Die Bundesregierung hat im Laufe des Berichtsjahres den Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes verabschiedet. Die erste Lesung im Bundesrat hat stattgefunden; der Deutsche Bundestag hat den Entwurf u. a. an den Innenausschuß überwiesen.

Die Bundesregierung hat im Laufe des bisherigen Verfahrens nur sehr wenige meiner gegenüber dem Bundesminister des Innern gemachten Vorschläge und Anregungen zu datenschutzrechtlichen Verbesserungen des Melderechtsrahmengesetzes (siehe auch 8. TB S. 10) übernommen. Von diesen Anregungen, die insbesondere auf Empfehlungen der Landesbeauftragten für den Datenschutz zurückgehen — die Länder sind bekanntlich für die Durchführung des Melderechts verantwortlich — greife ich für den Bericht zwei heraus, die für den Bürger von besonderer Bedeutung sind:

- In § 12 MRRG ist geregelt, welche Wohnung eines Einwohners, der mehrere Wohnungen hat, seine Hauptwohnung ist; u. a. heißt es in § 12 Abs. 1 MRRG: „Der Einwohner hat der Meldebehörde mitzuteilen, welche Wohnung seine Hauptwohnung ist." Dieser Satz soll in dem vorliegenden Entwurf gestrichen werden. Statt dessen erweitert der Entwurf § 12 um einen Absatz 4, der den Einwohner verpflichtet, Angaben zur Feststellung der Sachverhalte nach den Absätzen 2 und 3 zu machen. Damit würde eine neue Auskunftspflicht der Meldepflichtigen gegenüber der Meldebehörde begründet. Hiernach könnte die Meldebehörde sehr sensible Angaben bei einem Betroffenen erfragen, um Anhaltspunkte und Gründe für die vorwiegende Benutzung einer Wohnung zu erhalten (z. B. dauerndes Getrenntleben von der Familie oder Entscheidungen über das Personensorgerecht). Ich halte die gegenwärtige Regelung für ausreichend. Mir sind keine Gründe bekannt geworden, die eine solche Erweiterung der Auskunftspflicht gegenüber den Meldebehörden rechtfertigen.
- Im Zusammenhang mit den im Jahre 1989 durchgeführten Wahlen, wurde ich von verschiedenen Seiten gefragt, welche Möglichkeiten ein Bürger hat, sich gegen Wahlwerbung zu schützen, insbesondere wenn der sogenannten Wahlwerbung Kauf- und Abonnementsaufforderungen beigefügt sind, die über das hinausgehen, was als eigentliche Wahlwerbung — nämlich Darstellung der politischen Ziele einer Partei — zu verstehen ist. Meine Position, die sich auch in den Landesmeldegesetzen von Bayern und Berlin findet, den betroffenen Bürgern ein Widerspruchsrecht gegen solche Auskünfte einzuräumen, versteht sich vor folgendem Hintergrund: Nach § 22 Abs. 1 MRRG dürfen die Meldebehörden Parteien und Wählergruppen im

Zusammenhang mit Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, akademische Grade und Anschriften von Wahlberechtigten erteilen. Für die Zusammensetzung dieser sogenannten Melderegisterauskunft in besonderen Fällen ist das Lebensalter der Betroffenen bestimmend; die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden. Nach dieser Vorschrift kann sich kein betroffener Bürger einer solchen Wahlwerbung entziehen, wenn Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament anstehen. Bei der Vielgestaltigkeit unserer Parteienlandschaft ist es den Meldebehörden und den Innenministerien der Länder kaum möglich, die Einhaltung der Zweckbestimmung dieser Daten zu kontrollieren. Jede für eine Wahl zugelassene Partei kann somit — so auch die Auffassung des Bundesministers des Innern — von jeglicher Meldebehörde eine Auskunft erlangen, die sich auf *alle* Wahlberechtigten bezieht. Eine im ganzen Bundesgebiet zugelassene Partei könnte sich somit beinahe ein komplettes Register aller Bundesbürger anlegen. Nach dem Melderechtsrahmengesetz und den Landesmeldegesetzen darf sie diese Daten zwar nur für den Zweck der Wahlwerbung verwenden. Eine Kontrolle der Einhaltung dieser Zweckbindung kann aber außerordentlich schwierig sein, z. B. bei einer Partei, die sich nach einer Wahl wieder auflöst.

Der Bundesminister des Innern hat mir mittlerweile signalisiert, daß er sich einer Erweiterung des § 22 Abs. 1 MRRG um ein Widerspruchsrecht der Bürger nicht widersetzen würde, wenn eine solche Ergänzung des Melderechtsrahmengesetzes in den Beratungen der Ausschüsse des Deutschen Bundestages vorgeschlagen werden sollte.

Ich werde diese und weitere Überlegungen zur datenschutzrechtlichen Verbesserung des Melderechtsrahmengesetzes in die Ausschußberatungen des Deutschen Bundestages einbringen.

3.2 Ausländerzentralregister

3.2.1 Kontrolle beim Ausländerzentralregister

Aufgrund der Eingabe eines Bürgers habe ich beim Ausländerzentralregister kontrolliert, ob Daten des Petenten, der mittlerweile die deutsche Staatsangehörigkeit erworben hatte, noch im Ausländerzentralregister (AZR) gespeichert waren. Dies war nicht der Fall.

Im Zusammenhang hiermit habe ich mich auch mit dem Benachrichtigungsverfahren befaßt, in dem das AZR zwecks Löschung im Register über die Einbürgerung eines Ausländers unterrichtet wird. Nach Nr. 5.21 der Verwaltungsbestimmungen über den Verkehr zwischen den Ausländerbehörden und dem Bundesverwaltungsamt hat die Ausländerbehörde das AZR über den Erwerb der deutschen Staatsangehörigkeit oder der Rechtsstellung als Deutscher im Sinne des Artikel 116 Abs. 1 GG zu unterrichten. Um die Wirksamkeit des Benachrichtigungsverfahrens kontrollieren zu können, habe ich gemeinsam mit dem Bundesverwaltungsamt ein zeitlich begrenztes Prüfprogramm zur Feststellung von Fällen entwickelt, in denen mangels Mitteilung an das AZR die Daten eingebürgerter Ausländer dort nicht gelöscht worden sind. Die Auswertung hat eine unbefriedigend hohe Fehlerquote ergeben. Von den 600 ausgesuchten Einzelfällen war in 34 Fällen keine Mitteilung an das AZR erfolgt. An der Auffassung des Bundesverwaltungsamtes, mit der im Rahmen des neuen AZR vorgesehenen Datenfernübertragung von den Ausländerbehörden an das AZR lasse sich diese Fehlerrate verringern, habe ich Zweifel geäußert. Ich habe vielmehr empfohlen zu prüfen, ob nicht das bislang über zwei Etappen führende Informationsverfahren (Meldung der Einbürgerungsbehörde an die Ausländerbehörde, sodann Mitteilung der Ausländerbehörde an das AZR) durch ein einstufiges Verfahren, nämlich der direkten Meldung der Einbürgerungsbehörde an das AZR, ersetzt werden muß. Zudem halte ich die Mitteilung an das AZR für so bedeutsam, daß sie in einer Rechtsnorm geregelt werden sollte. Eine Äußerung des Bundesministers des Innern zu dieser Problematik liegt mir bisher noch nicht vor.

Ebenfalls durch die Eingabe eines Bürgers bin ich darauf aufmerksam geworden, daß für eine Auskunft aus dem Ausländerzentralregister eine Gebühr von 10,00 DM erhoben worden war. Dies ist zwar nach der Datenschutzgebührenordnung möglich, jedoch hat der Bundesminister des Innern den obersten Bundesbehörden schon 1979 geraten, bei der Erhebung der Gebühren von der Ausnahmeregel des § 3 der Datenschutzgebührenordnung großzügig Gebrauch zu machen. Danach kann auf die Gebühr von 10,00 DM verzichtet werden, wenn es sich z. B. um eine einfache schriftliche Auskunft handelt.In dem mir bekannt gewordenen Fall habe ich erreicht, daß dem Petenten die bereits entrichtete Gebühr erstattet worden ist. Insofern begrüße ich auch, daß im Rahmen der Novellierung des Bundesdatenschutzgesetzes die klare Regelung vorgesehen wird, daß eine Gebühr für die Auskunftserteilung von Behörden und sonstigen öffentlichen Stellen an den Betroffenen nicht mehr erhoben wird.

3.2.2 Regierungsentwurf eines Gesetzes über das Ausländerzentralregister

Die Bundesregierung hat im August 1989 den Regierungsentwurf eines Gesetzes über das Ausländerzentralregister (AZR-Gesetz, BT-Drucksache 11/5828) beschlossen. Ein Vergleich dieses Entwurfs mit dem früheren Referentenentwurf, zu dem ich die wichtigsten datenschutzrechtlichen Kritikpunkte in meinem Elften Tätigkeitsbericht (S. 16f.) verdeutlicht habe, läßt erkennen, daß meine Vorschläge weitgehende Berücksichtigung gefunden haben. Unabhängig hiervon bleibt es freilich bei der schon in meinen früheren Berichten (9. TB S. 15f., 11. TB S. 16f.) getroffenen Aussage, daß es ergänzend zu den registerrechtlichen Vorschriften auch der Beseitigung von datenschutzrechtlichen Defiziten im Bereich des Ausländerrechts bedarf. Dies gilt namentlich für die auch von den Lan-

desbeauftragten für den Datenschutz immer wieder artikulierten Fragen, welche Ereignisse Einreisebedenken begründen und in welcher Weise AZR-Auskünfte, in denen Einreisebedenken vermerkt sind, verwertet werden dürfen.

Positive Erwähnung verdient, daß der Bundesminister des Innern meiner Forderung nach notwendiger Ergänzung des Entwurfs um Regelungen über die Löschung gespeicherter Daten durch Einfügung einer Vorschrift über „Berichtigung, Löschung und Sperrung von Daten" entgegengekommen ist. Wichtig ist dabei besonders die ausdrückliche Klarstellung, daß Daten von der Registerbehörde zu löschen sind, wenn der Betroffene die deutsche Staatsangehörigkeit erworben hat oder sich nach der Speicherung seiner Daten herausstellt, daß er Deutscher im Sinne des Artikels 116 Abs. 1 des Grundgesetzes ist (vgl. oben 3.2.1). Desgleichen folgt der Regierungsentwurf meinen Empfehlungen, zum Zwecke datenschutzrechtlicher Kontrolle wie auch der Berichtigung unrichtiger AZR-Auskünfte (z. B. nach Berichtigung eines unrichtig mitgeteilten und gespeicherten Datums durch die mitteilende Ausländerbehörde) eine Protokollierung von Datenübermittlungen vorzusehen. Die vorgesehene Regelung umfaßt sowohl Auskünfte, die im herkömmlichen Verfahren als auch solche, die automatisiert erteilt werden. Positiv ist, daß auf die in meinem Elften Tätigkeitsbericht zitierte und kritisierte Regelung verzichtet wurde, die Aussiedler mit der Vermutung belastet, Ausländer zu sein, wenn ihr Status nach sechs Monaten noch nicht festgestellt ist.

Die Regelung über Abrufe im automatisierten Verfahren betrachte ich als einen Kompromiß. Das zweistufige Konzept enthält einen Maximalkatalog von Behörden, die zum automatisierten Abrufverfahren zugelassen werden können, unterwirft in diesem Rahmen aber jede einzelne Behörde einem Zulassungsverfahren nach Kriterien, die aufgrund meiner Empfehlungen in den Entwurf Eingang gefunden haben. Voraussetzung für die Einrichtung eines automatisierten Abrufverfahrens im Einzelfall ist, daß es wegen der „Vielzahl der Übermittlungsersuchen" oder wegen „der besonderen Eilbedürftigkeit unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen" angemessen ist. Außerdem müssen die „zur Datensicherung erforderlichen technischen und organisatorischen Maßnahmen" ergriffen worden sein. Diese Beschränkungen sollten — hierfür enthält der Regierungsentwurf eine Verordnungsermächtigung — im Rahmen der in Vorbereitung befindlichen Verordnung zur Durchführung des AZR-Gesetzes präzisiert werden, um — besonders von Landesbeauftragten für den Datenschutz geäußerte — Befürchtungen auszuräumen, von den Möglichkeiten des automatisierten Abrufs könne in einem unangemessenen und nicht erforderlichen Maße Gebrauch gemacht werden.

Kritik an dem Regierungsentwurf habe ich in bezug auf eine Regelung geltend gemacht, die für nicht mit grenzpolizeilichen Aufgaben betraute sonstige Polizeivollzugsbehörden sowie für Behörden der Staatsanwaltschaft die Möglichkeit vorsieht, über im Register näher beschriebene Standarddaten des Betroffenen hinaus die im Register gespeicherten „weiteren Daten" im automatisierten Verfahren abzurufen (§ 10 Abs. 2 i. V. m. § 16 des Regierungsentwurfs). Die Regelung des Entwurfs begegnet deshalb Bedenken, weil einerseits § 10 Abs. 2 davon ausgeht, daß die über die Grunddaten hinausgehenden Daten nur dann für die in § 10 Abs. 1 genannten Stellen erforderlich sind, wenn die Grunddaten zur Aufgabenerfüllung nicht ausreichen, was nur im Einzelfall geprüft werden kann. Andererseits unterläge die abrufberechtigte Stelle, wenn sie online abrufen kann, allenfalls einer nachträglichen Kontrolle. Die Stellungnahme des Bundesrates zu § 10 des Regierungsentwurfs (Nr. 18) bringt leider keine Verbesserung, sondern eine datenschutzrechtliche Verschlechterung. Die Übermittlung der im Register gespeicherten Daten — also nicht nur der Grunddaten — soll danach zur durchgängigen Routine der Antwort auf Auskunftsersuchen dieser Behörden (und zusätzlich der Gerichte) werden. Ich trete für eine gut kontrollierbare differenzierende Lösung ein, die unter Gesichtspunkten des Datenschutzes wie auch der Praktikabilität den automatisierten Abruf auf die Informationen beschränkt, die die genannten Behörden tatsächlich in der Regel brauchen.

3.3 Neuregelung des Ausländerrechts

Auf die Notwendigkeit, Eingriffe in das informationelle Selbstbestimmungsrecht von Ausländern auf klarere rechtliche Grundlagen zu stellen und datenschutzrechtliche Defizite nicht nur im Bereich des Ausländerzentralregisters, sondern auch im materiellen Ausländerrecht aufzuarbeiten, habe ich schon seit Jahren hingewiesen (vgl. 11. TB S. 16f. sowie oben 3.2.2). Als eine Gelegenheit, nunmehr wesentliche Verbesserungen zu erreichen, betrachte ich den Entwurf für ein Gesetz zur Neuregelung des Ausländerrechts. Wenn die engen Fristen für eine Äußerung zu diesem mir Ende September 1989 zugegangenen Entwurf auch kaum Möglichkeiten für die notwendige Abstimmung mit den Landesbeauftragten für den Datenschutz ließen, so läßt sich in vorläufiger Bewertung doch feststellen, daß die in der ursprünglichen Fassung des Entwurfs zunächst unzureichenden datenschutzrechtlichen Regelungen aufgrund meiner Stellungnahmen sowie eines intensiven Dialogs mit dem Bundesminister des Innern, in den auch andere Ressorts einbezogen waren, inzwischen deutliche Verbesserungen erfahren haben.

Besonders zu nennen sind:

— Das Prinzip, daß personenbezogene Informationen in erster Linie beim Betroffenen selbst zu erheben sind.

  Der Dialog mit dem Betroffenen soll also den Vorrang vor der Informationsgewinnung bei anderen Stellen haben.

— Vermehrte Transparenz.

  Die Rechte des Betroffenen, über seine personenbezogenen Daten Auskunft zu erhalten und über Informationsflüsse an Dritte informiert zu werden, sollen verstärkt werden.

— Deutlichere Zweckbindung.

Personenbezogene Informationen sollen grundsätzlich nur der Ausführung des vorgesehenen Gesetzes und ausländerrechtlicher Bestimmungen in anderen Gesetzen dienen.

— Verbesserter Schutz besonderer Geheimhaltungsinteressen, wie Arztgeheimnis, Sozialgeheimnis, Steuergeheimnis etc.

Das Prinzip, daß bei der Informationsgewinnung entsprechende gesetzliche Verwendungsregelungen zu beachten sind, soll ausdrücklich festgelegt werden. Durchbrechungen sollen im überwiegenden Allgemeininteresse nur in sehr engen im Gesetz selbst präzis bestimmten Ausnahmefällen zulässig sein.

Inzwischen ist der Gesetzentwurf vom Bundeskabinett beschlossen und dem Bundesrat zugeleitet worden. Ich werde die weiteren Beratungen mit Aufmerksamkeit verfolgen.

3.4 Gesundheitsdaten von Asylbewerbern

Im Zehnten und Elften Tätigkeitsbericht (S. 15 bzw. S. 16) habe ich zu der Frage einer ausreichenden Rechtsgrundlage für routinemäßige ärztliche Untersuchungen von Asylbewerbern berichtet. Nach Mitteilung des Bundesministers für Jugend, Familie, Frauen und Gesundheit hat der damit befaßte Ausschuß für Seuchenhygiene inzwischen einen Bericht über den erforderlichen Umfang von Untersuchungen und einen darauf gestützten Vorschlag vorgelegt; der Bericht ist in einem nächsten Schritt von der Arbeitsgemeinschaft der Leitenden Medizinalbeamten der Länder zu beraten.

Nach dem Bericht ist es *in der Regel* erforderlich, aber auch ausreichend, dem Asylbewerber ein Programm von Untersuchungen anzubieten, das nur mit Einwilligung des Betroffenen durchgeführt wird. Das Programm soll Untersuchungen auf übertragbare Krankheiten und — aus fürsorgerischen Gründen — auch Untersuchungen hinsichtlich anderer Krankheiten enthalten, deren Erkennung grundsätzlich allein im Interesse des Asylbewerbers liegt. Routinemäßige HIV-Untersuchungen werden entsprechend dem Beschluß der 59. Gesundheitsministerkonferenz vom 17./18. November 1988 nicht als erforderlich angesehen. Im Hinblick auf die Einwilligung soll der Asylbewerber in geeigneter Form über die Freiwilligkeit sowie über Zweck und Umfang der Untersuchungen informiert werden.

Ergänzend verweist der Bericht darauf, daß *im Einzelfall* bei Vorliegen bestimmter Voraussetzungen sowohl die Gesundheitsbehörde nach dem Bundesseuchengesetz als auch die Ausländerbehörde auf der Grundlage des Asylverfahrensgesetzes verpflichtende Anordnungen zu ärztlichen Untersuchungen des Asylbewerbers treffen kann.

Aus der Sicht des Datenschutzes ist es erfreulich, daß der Umfang der ärztlichen Untersuchungen, d. h. der Eingriff in das informationelle Selbstbestimmungsrecht des Asylbewerbers, unter dem Gesichtspunkt der Erforderlichkeit eingegrenzt wird und die Entscheidung über die Durchführung dieser Untersuchungen weitgehend bei dem Betroffenen selbst verbleiben soll. Ich gehe dabei davon aus, daß der Asylbewerber das jeweils angebotene Untersuchungsprogramm nicht nur vollständig akzeptieren oder ablehnen kann, sondern seine Einwilligung auch auf Teile des Untersuchungsprogramms beschränken darf. Vor seiner Entscheidung ist der Asylbewerber ausreichend zu unterrichten und — auch dies empfiehlt der Bericht — dabei insbesondere darauf hinzuweisen, daß die Ergebnisse der Untersuchungen keinen Einfluß auf das Asylverfahren haben.

Soweit der Bericht als Grundlage für die Anordnung von zwangsweisen Untersuchungen den § 20 Abs. 1 Satz 2 Asylverfahrensgesetz nennt, verweise ich auf meinen Zehnten Tätigkeitsbericht (S. 15), in dem ich vorgeschlagen habe, im Hinblick auf das Gebot der Normenklarheit präzisere Gesetzesvorschriften für etwa erforderliche zwangsweise ärztliche Untersuchungen zu schaffen.

3.5 Neue Personalausweise und Pässe

3.5.1 Datenübermittlung an die Bundesdruckerei

Die Einhaltung datenschutzrechtlicher Vorschriften durch Bundesbehörden im Verfahren der Beantragung und Herstellung neuer Personalausweise und Pässe war für mich auch im zurückliegenden Jahr ein wichtiges Thema. Bei einer Kontrolle der Bundesdruckerei habe ich erneut (s. 11. TB S. 18) festgestellt, daß der Bundesdruckerei Anträge auf Ausstellung von Personalausweisen und Pässen zugehen, die oftmals personenbezogene Daten enthalten, die zwar für die Ausweisbehörden, nicht aber für die Bundesdruckerei von Bedeutung sind. Darauf habe ich den Bundesminister des Innern hingewiesen und ihn gebeten, in Kontakten mit den Innenverwaltungen der Länder für Abhilfe zu sorgen. Bedauerlicherweise hält der Minister an seinem Standpunkt fest, es handele sich nicht um Datenübermittlungen von Ausweisbehörden an die Bundesdruckerei. Die Bundesdruckerei produziere die Personalausweise und Reisepässe — so drückt er sich aus — nur als „Schreibmaschine" *im Auftrag* der Personalausweis- und Paßbehörden der Länder. Ihre Verantwortung erschöpfe sich in der drucktechnischen Qualität des für die zuständigen Behörden herzustellenden Ausweispapiers, während die Personalausweis- und Paßbehörden als ausstellende Behörden die alleinige Verantwortung für Richtigkeit und Vollständigkeit der Ausweisdokumente trügen.

Von einer Datenverarbeitung im Auftrag könnte aber — wie ich schon in meinem Elften Tätigkeitsbericht (S. 18f.) näher aufgeführt habe — nur dann ausgegangen werden, wenn sich der Auftrag ausschließlich auf die Verarbeitung personenbezogener Daten bezöge. Nach dem Willen des Gesetzgebers ist der Bundesdruckerei die Herstellung der Personalausweise und Pässe aber in eigener Verantwortung übertragen worden. Eine Übermittlung von Daten, die sie zu dieser Aufgabenerfüllung nicht benötigt, ist mit dem Grundsatz der Erforderlichkeit nicht vereinbar.

Diese Auffassung wird auch von den Landesbeauftragten für den Datenschutz geteilt. Sie haben die Innenminister ihrer Länder unterrichtet und entsprechende datenschutzrechtliche Empfehlungen gegeben. Der Bundesminister des Innern sollte — so empfehle ich — Bemühungen, hier Abhilfe zu schaffen, nachdrücklich unterstützen.

3.5.2 Rückgabe fehlerhafter Ausweise an die Bundesdruckerei

Nach Ziffer 6.7.3 der Allgemeinen Verwaltungsvorschriften zur Durchführung des Paßgesetzes hat die Paßbehörde bei fehlerhaft hergestellten Reisepässen den Antrag unter Vergabe einer neuen Seriennummer erneut an die Bundesdruckerei zu senden. Dabei sind in dem Antrag die bisherige Seriennummer durchzustreichen und der fehlerhafte Reisepaß beizufügen. Die Paßbehörde hat den fehlerhaften Reisepaß zuvor durch Abschneiden der linken unteren Ecke ungültig zu machen. Stellt die Bundesdruckerei fest, daß dies nicht geschehen ist, macht sie den Reisepaß unverzüglich nach Eingang ungültig. Die fehlerhaften und ungültigen Reisepässe werden von der Bundesdruckerei vernichtet. Über die Vernichtung ist eine Niederschrift anzufertigen. Zweck dieser unter meiner Mitwirkung geschaffenen Vorschrift ist sicherzustellen, daß zu einer Person nur *ein* gültiger Reisepaß besteht und kein falsches aber äußerlich korrektes Personaldokument in Umlauf kommt.

Im Rahmen der Kontrolle bei der Bundesdruckerei habe ich festgestellt, daß die Paßbehörden in zunehmendem Maße diese Vorschrift nicht beachten und den fehlerhaften Ausweis nicht an die Bundesdruckerei zurückgeben. Die Bundesdruckerei hat, um Nachteile für den Bürger zu vermeiden, zwar neue Reisepässe hergestellt und der Paßbehörde ausgeliefert, intern aber die fehlende Rückgabe dokumentiert.

Ich habe den BMI gebeten, in Kontakten mit den Innenressorts der Länder auf die Einhaltung der genannten Vorkehrungen zur Gewährleistung der datenschutzrechtlichen Prinzipien des Paßgesetzes hinzuwirken. Darüber hinaus habe ich ihn darauf hingewiesen, daß sich die Problematik nicht nur in bezug auf Reisepässe, sondern auch in Bezug auf Personalausweise stellt. Gleichzeitig habe ich die Landesbeauftragten für den Datenschutz auf diese Problematik aufmerksam gemacht.

Der Bundesminister des Innern ist meiner Empfehlung erfreulicherweise gefolgt und hat die Innenminister/-senatoren der Länder darauf hingewiesen, daß im Interesse eines lückenlosen Nachweises über den Verbleib aller in der Bundesdruckerei hergestellten Pässe und Personalausweise die Einhaltung dieser Regelungen unverzichtbar ist. Nach meinem bisherigen Kenntnisstand ist aber im Verhalten der Personalausweis- und Paßbehörden bislang keine Änderung eingetreten. Falls die Bemühungen auch der Landesbeauftragten für den Datenschutz nicht zu einer Verbesserung führen, wird zu erwägen sein, der Bundesdruckerei zu empfehlen, die Auslieferung des Zweitdokuments jeweils auszusetzen, bis ihr — den Verwaltungsvorschriften gemäß — das fehlerhafte Erstdokument zugegangen ist.

3.6 Zivildienst

3.6.1 Aufbewahrung von Anerkennungsunterlagen

Über Probleme der Aufbewahrung von Anerkennungsunterlagen der anerkannten Kriegsdienstverweigerer habe ich bereits mehrfach, zuletzt im Elften Tätigkeitsbericht (S. 19), berichtet.

Mit dem Zweiten Gesetz zur Änderung des Kriegsdienstverweigerungs-Neuordnungsgesetzes hat der Gesetzgeber nunmehr erfreulicherweise durch Ergänzung des § 2 des Kriegsdienstverweigerungsgesetzes eine gesetzliche Regelung über die Vernichtung der Akten des Anerkennungsverfahrens getroffen. Danach werden diese Akten, die die besonders schutzwürdigen Daten über die Gewissensentscheidung des Betroffenen enthalten, mit Ausnahme des Anerkennungsbescheides spätestens sechs Monate nach Ableistung des Zivildienstes vernichtet. In den Fällen, in denen ein anerkannter Kriegsdienstverweigerer nicht zum Zivildienst herangezogen wird, werden die Akten über die Anerkennungsverfahren nach Ablauf des Jahres, in dem er das 32. Lebensjahr vollendet hat, vernichtet.

Auch für diejenigen Kriegsdienstverweigerer, die vor dem Inkrafttreten dieser Regelung ihren Zivildienst abgeleistet haben, sieht das Gesetz Regelungen vor: Deren Akten über das Anerkennungsverfahren werden innerhalb von drei Jahren nach Inkrafttreten des Gesetzes vernichtet.

Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mich wissen lassen, das Bundesamt für den Zivildienst werde in Kürze in das Vernichtungsverfahren — über den gesetzlich vorgeschriebenen Umfang hinaus — auch die Aktenvorgänge einbeziehen, die von den Kreiswehrersatzämtern übersandt worden sind (z. B. Unterlagen über das Musterungsverfahren), also zeitlich vor dem Beginn des Zivildienstes liegen.

3.6.2 Arbeitsberichte von Zivildienstleistenden

In meinem Elften Tätigkeitsbericht (S. 19) habe ich empfohlen, die für Zivildienstleistende in der Individuellen Schwerstbehindertenbetreuung entwickelten Grundsätze auch für Kriegsdienstverweigerer bei den Mobilen Sozialen Hilfsdiensten zu übernehmen. Diese Prinzipien stellen sicher, daß im Interesse des Schutzes der Privatsphäre der Betreuten die Zivildienstleistenden keine Angaben über die Art der einzelnen Betreuungsleistungen, sondern nur über den benötigten Zeitaufwand zu machen haben. Der Bundesminister für Jugend, Familie, Frauen und Gesundheit hat mir mitgeteilt mit der Arbeitsgemeinschaft der Freien Wohlfahrtspflege sei vereinbart worden, daß neben den in den Einsatzstellen geführten Wochendienstplänen über den Einsatz der Zivildienstleistenden im Mobilen Sozialen Hilfsdienst Aufzeichnungen

über die Art der von ihnen bei den Betreuten geleisteten Verrichtungen nicht erfolgen. Ich begrüße diese Entscheidung.

3.7 Bundesanstalt Technisches Hilfswerk

In meinem Elften Tätigkeitsbericht (S. 18f.) habe ich über Ergebnisse einer datenschutzrechtlichen Kontrolle bei der Bundesanstalt Technisches Hilfswerk berichtet. Der Bundesminister des Innern hat mich inzwischen über die aufgrund meiner Empfehlungen eingeleiteten oder bereits durchgeführten Maßnahmen informiert. Besonders zu erwähnen sind folgende Punkte:

Inzwischen ist ein Grobkonzept für IT-Einsatzmöglichkeiten im nachgeordneten Bereich des THW erarbeitet worden. Dieses Konzept enthält auch erste Vorschläge zum „Sicherungs- und Datenschutzkonzept" sowie Hinweise zur wirtschaftlich sinnvollen Integration bereits vorhandener Hard- und Softwareausstattung. Im Jahr 1990 ist als zweiter Schritt die Erstellung des Feinkonzepts vorgesehen. Darin soll auch der zur Lehrgangsbeschickung erforderliche Datenumfang, den ich in meinem Elften Tätigkeitsbericht angesprochen habe, untersucht werden.

Im Rahmen von Lehrgängen sind die Hauptsachgebietsleiter der Verwaltung der Landesverbände sowie die Geschäftsführer mit den Anforderungen des Bundesdatenschutzgesetzes vertraut gemacht worden. Auch dies entspricht einer meiner Empfehlungen.

Erfreulich ist auch, daß — meinen Vorschlägen folgend —, die Helfer nunmehr bei der Abgabe ihrer Verpflichtungserklärung über ihre Einsichtsrechte in ihre jeweilige beim THW geführte Helferakte informiert werden.

Auch in rechtlicher Hinsicht sind Fortschritte zu verzeichnen: Im Rahmen der Vorbereitung des THW-Helferrechtsgesetzes habe ich erreicht, daß Regelungen über die Erhebung, Verwendung und Zweckbindung der personenbezogenen Daten der Helfer in das Gesetz aufgenommen worden sind.

4 Rechtswesen

4.1 Strafprozeßordnung

Bemühungen des Bundesministers der Justiz um die Schaffung von den Anforderungen des Bundesverfassungsgerichts genügenden Vorschriften für den Umgang mit personenbezogenen Daten im Strafverfahren bildeten auch im Berichtsjahr einen Schwerpunkt im Rahmen meiner Beratungsaufgaben bei Rechtsetzungsvorhaben (vgl. 9. TB S. 19f., 10. TB S. 22, 11. TB S. 20). Zu dem Referentenentwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts — Strafverfahrensänderungsgesetz 1988 — hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die wesentlichen Kritikpunkte in einer Entschließung deutlich gemacht, die als Anlage 3 zu diesem Bericht abgedruckt ist. Darüber hinaus habe ich dem Bundesminister der Justiz — der Ankündigung in meinem Elften Tätigkeitsbericht entsprechend — zur Konkretisierung und Vertiefung meiner Vorstellungen eine eingehende Stellungnahme zugehen lassen.

Nach im April 1989 durchgeführten Erörterungen mit Vertretern von Justiz- und Innenressorts der Länder, an denen auch ich beteiligt war, hat mir der Bundesminister der Justiz im Juni 1989 den Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts — Strafverfahrensänderungsgesetz 1989 — zugesandt, der gleichzeitig den Bundesressorts zur Vorabstimmung und Vorbereitung eines Kabinettbeschlusses zugegangen ist. Dieser Entwurf folgt — unbeschadet einer Reihe von Einzelpunkten, zu denen ich schriftliche Stellungnahmen abgegeben habe — nach meiner Einschätzung im wesentlichen den Vorentwürfen. Die zentrale Frage ist nach wie vor, wie angesichts zunehmend komplexerer Fahndungsmethoden und wachsender Mittel und Möglichkeiten der modernen Datenverarbeitung ein angemessener Ausgleich zwischen den Interessen an vollständiger Straftatenermittlung und Durchsetzung des staatlichen Strafanspruchs einerseits sowie dem Recht auf informationelle Selbstbestimmung andererseits gefunden werden kann. Das Problem stellt sich in besonderem Maße dort, wo durch die Datenverarbeitung in Rechte Dritter eingegriffen wird, die weder Beschuldigte noch Verdächtigte des Strafverfahrens sind. In einer Reihe von Punkten besteht der Eindruck, daß der Entwurf nachzuvollziehen sucht, was die Praxis in den vergangenen Jahren an neuen Instrumenten entwickelt hat. Dabei bedarf die Frage nach den bereits erkennbaren oder mit einiger Sicherheit zu erwartenden Erfolgen der Anwendung dieser Instrumente — und damit nach deren Erforderlichkeit im überwiegenden Allgemeininteresse — noch vertiefter Prüfung. Ansätze für die notwendige Flurbereinigung im Bereich der polizeilichen und staatsanwaltschaftlichen Dateien sollten nicht durch eine Konzeption des Nebeneinanders und damit der Verdoppelung oder Vervielfachung der Speicherung von sensiblen Daten im Bereich der Strafrechtspflege zunichte gemacht werden.

Angesichts von in der öffentlichen Diskussion erkennbaren Widerständen verschiedener Seiten gegen den Entwurf möchte ich — unbeschadet eines auch von mir gesehenen weiteren Diskussionsbedarfs — die dringende Notwendigkeit der Schaffung geeigneter gesetzlicher Regelungen erneut betonen. Bürger wie Strafverfolgungsbehörden benötigen möglichst bald Klarheit über die bei der Strafverfolgung zulässigen Verfahren und Methoden.

4.2 Zivilprozeßordnung

4.2.1 Mehrzahl von Drittschuldnern

In meinem Zehnten Tätigkeitsbericht (S. 23f.) habe ich über die datenschutzrechtliche Problematik berichtet, die entsteht, wenn Pfändungs- und Überweisungsbeschlüsse gleichzeitig an mehrere Drittschuldner gerichtet sind. Durch die gemeinsame Nennung in einem Beschluß erfahren z. B. der Kunde eines Lieferanten oder der Patient eines Arztes davon, daß For-

derungen auch gegen die anderen in dem Beschluß genannten Personen (Drittschuldner) bestehen, ohne daß dies von der Sache her erforderlich ist. Meine Diskussion hierzu mit dem Bundesminister der Justiz dauert noch an. In ihrer Stellungnahme zu dieser auch in meinem Elften Tätigkeitsbericht (S. 21) angesprochenen Thematik teilt die Bundesregierung mit, sie werde bei der Überarbeitung des Zwangsvollstreckungsrechts in einer Arbeitsgruppe aus Vertretern von Landesjustizverwaltungen unter Beteiligung des Bundesministers der Justiz „datenschutzfeste gesetzliche Regelungen" über Pfändungs- und Überweisungsbeschlüsse bei einer Mehrzahl von Drittschuldnern zur Erörterung stellen. Sie führt ergänzend aus, die Landesjustizverwaltungen befürworteten eine „datenschutzfeste Festschreibung der bisher geübten Praxis".

Die bisher geübte Praxis ist mit § 829 ZPO nicht vereinbar; dieser spricht klar und eindeutig von „dem Drittschuldner". Eine Aufnahme einer Mehrzahl von Drittschuldnern in *einen* Pfändungs- und Überweisungsbeschluß ist daher von dieser Vorschrift nicht gedeckt. Nur ein solches Verständnis des § 829 ZPO entspricht den Anforderungen des Volkszählungsurteils. Die durch das gegenwärtige Verfahren bedingte Unterrichtung der Drittschuldner über andere Drittschuldner und ihre Beziehungen zum Schuldner enthält jeweils einen empfindlichen Eingriff in das informationelle Selbstbestimmungsrecht der anderen Drittschuldner. Ich habe dem Bundesminister der Justiz daher dringend empfohlen, auf eine Änderung der derzeitigen Praxis hinzuwirken und im Falle einer Novellierung der Zivilprozeßordnung die Unzulässigkeit des bisher geübten Verfahrens im Gesetz zu verdeutlichen und nicht, wie die Stellungnahme der Bundesregierung erwarten läßt, die bisherige auch verfassungsrechtlich bedenkliche Praxis zu bestätigen. Eine Reaktion des Bundesministers der Justiz hierzu liegt mir noch nicht vor.

4.2.2 Befugnisse der Gerichtsvollzieher

Von dem Regierungsentwurf eines Rechtspflege-Vereinfachungsgesetzes habe ich erst durch Drucksachen des Bundesrates und des Bundestages Kenntnis erhalten. Da der Entwurf Regelungen enthält, die das informationelle Selbstbestimmungsrecht berühren, bedauere ich im Hinblick auf mein Beratungsrecht nach § 19 Abs. 1 Satz 1 BDSG, nicht schon früher beteiligt worden zu sein.

Dies gilt namentlich für die vorgesehene Ergänzung der Zivilprozeßordnung durch einen neuen § 806 a (in der Fassung der BT-Drucksache 11/3621). Hiernach hat bei erfolglosen Pfändungsversuchen der Gerichtsvollzieher u. a. Kenntnisse von Geldforderungen des Schuldners, die er „anläßlich der Zwangsvollstrekkung durch *Befragung des Schuldners*" erhalten hat, dem Gläubiger mitzuteilen. Die vorliegende Fassung unterstellt ein Recht des Gerichtsvollziehers, den Schuldner nach Geldforderungen gegen Dritte zu befragen und regelt die Verwendung dieser Information. Die Befugnis selbst wird nach meinem Verständnis durch diese Vorschrift nicht geschaffen. Die Entwurfsbegründung deutet mit dem Hinweis, „in der Praxis" werde der Schuldner „in diesen Fällen vom Gerichtsvollzieher ... gefragt" darauf hin, daß eine besondere Befugnisnorm nicht besteht. Offen bleibt auch, ob der angestrebten Möglichkeit zu fragen, eine Pflicht des Schuldners zu antworten entsprechen soll. Dem Bundesminister der Justiz habe ich empfohlen, sich in den weiteren parlamentarischen Beratungen dafür einzusetzen, die Ermittlungsbefugnisse des Gerichtsvollziehers normenklar zu regeln. Die Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates zu dieser Vorschrift läßt mich davon ausgehen, daß jedenfalls in dieser Zielsetzung Einvernehmen besteht. Darüber hinaus halte ich an meiner Empfehlung fest, daß die Gesetzesvorschrift erkennen lassen sollte, ob neben dem Fragerecht des Gerichtsvollziehers eine Antwortpflicht des Gefragten bestehen soll. Zwischenzeitlich geführten Gesprächen mit dem Bundesminister der Justiz habe ich entnommen, daß in Abstimmung mit anderen Ressorts ein neuer Formulierungsvorschlag zur Fassung des § 806a ZPO erarbeitet wird, der mir bei Redaktionsschluß des Tätigkeitsberichts noch nicht vorlag.

4.2.3 Befugnisse gerichtlicher Sachverständiger

Als einen weiteren Problembereich, in dem es einer dringenden Überarbeitung und Ergänzung zivilprozessualer Vorschriften bedarf, habe ich bereits in meinem Elften Tätigkeitsbericht (S. 21f.) die Befugnisse von gerichtlichen Sachverständigen zur Feststellung der Identität zu untersuchender Personen angesprochen. Der Bundesminister der Justiz hat diese Thematik zwischenzeitlich mit den Landesjustizverwaltungen erörtert. Diese halten — so hat er mich unterrichtet — im Hinblick auf die Tragweite der im Abstammungsprozeß zu treffenden Entscheidungen zur Abwehr und Aufklärung von Täuschungsversuchen ein *Lichtbild* der untersuchten Person zum Zwecke der sicheren Identifizierung für unerläßlich. Nach meinem Verständnis ist die Frage offen, ob dieses Konzept mit der Aufgabe der bisherigen Praxis der *Finger- oder Fußabdrücke* zur Identitätssicherung zu verbinden ist, oder ob etwa insoweit eine kumulative Identitätssicherung, wie sie der Bundesminister der Justiz ins Auge gefaßt hat, erforderlich ist. Er führt zu dieser Problematik aus, sich allein auf ein Lichtbild zu stützen, „dürfte Schwierigkeiten bereiten, zumal in der Praxis fast ausschließlich Sofortbildkameras Verwendung finden, bei denen eine zufriedenstellende Bildqualität nicht stets gewährleistet ist." Wenn das zutrifft, stellt sich die Frage, ob ein solches Lichtbild für das angestrebte Ziel der Identitätssicherung überhaupt geeignet ist.

Das Vorhaben des Bundesministers der Justiz, für den Abstammungsprozeß durch Ergänzung des § 372a ZPO eine ausdrückliche Regelung für die gutachterlichen Befugnisse zur Prüfung und Sicherung der Identität der zu untersuchenden Person zu schaffen, folgt im Ansatz meinen Empfehlungen. Dabei reicht es aber nicht aus, eine Pflicht der zu untersuchenden Person vorzusehen, *„die erforderlichen Maßnahmen* einschließlich der Aufnahme von Finger- oder Fußabdrücken zu dulden". Gerade die vom Bundesminister der Justiz wiedergegebene Erörterung mit den Lan-

desjustizverwaltungen über die Erforderlichkeit und Eignung der Mittel zeigt, daß die Wahl der „erforderlichen Maßnahmen" nicht der Rechtsanwendung in der Praxis, insbesondere nicht dem einzelnen Gutachter, überlassen bleiben darf. Aufnahme und Entgegennahme eines Lichtbildes durch eine staatliche Stelle gegen den Willen des Betroffenen sind Eingriffe in das Recht auf informationelle Selbstbestimmung, für die eine *ausdrückliche* gesetzliche Grundlage bestehen muß. Dies gilt erst recht dann, wenn nicht eine staatliche Stelle, sondern ein Gutachter die Maßnahmen aufgrund eines gerichtlichen Auftrages durchführen soll.

Nach wie vor gilt auch meine Empfehlung, den behandelten Fragen nicht nur in bezug auf die Zivilprozeßordnung, sondern auch in bezug auf andere Verfahrensordnungen nachzugehen (vgl. 11. TB S. 22). Der Bundesminister der Justiz hat ausgeführt, im Strafverfahren seien die Verpflichtungen des Beschuldigten und Dritter zur Duldung von Maßnahmen der Identitätsfeststellung „ausdrücklich nur in allgemeiner Form geregelt". Er verweist hierzu auf §§ 81b 1. Alternative und 163b StPO. Ich vermag hierin keine normenklaren Regelungen der Befugnisse von Sachverständigen zu sehen, zur Identitätssicherung bei der Erstellung von Blutgruppengutachten Lichtbilder und Fingerabdrücke aufzunehmen.

Einer Erörterung des Rechtspflege-Vereinfachungsgesetzes (§ 407a Abs. 4 i. d. F. der vorgesehenen Einfügung in die ZPO, BT-Drucksache 11/3621) mit dem Bundesminisster der Justiz habe ich entnommen, daß *Aufbewahrungsfristen* für personenbezogene Daten (Protokollbücher mit Befunden, Durchschriften der Gutachten und der Niederschriften) *beim Gutachter* nach Erstattung des Gutachtens nicht schon im Rahmen dieses Gesetzes bestimmt werden sollen. Soweit der Bundesminister der Justiz dabei auf vergleichbare Fragen der Aufbewahrung von Krankenunterlagen durch Ärzte hingewiesen hat, sehe ich eine Besonderheit der vorliegenden Problematik darin, daß den Befugnissen zum Zwangseingriff, mit denen gerichtliche Gutachter ausgestattet sind, nicht lediglich eine privatrechtliche, sondern eine gerichtsverfahrensrechtliche Verantwortung für den Schutz der erhobenen Daten entsprechen muß, weil der Gutachter „Hilfsorgan" des Richters ist. Zu bedenken ist auch, daß die in den Berufsordnungen für Ärzte festgelegten Aufbewahrungsfristen für Patientenunterlagen sich nur an *behandelnde* Ärzte richten und daß in dem hier fraglichen Bereich auch Nicht-Mediziner (z. B. Molekularbiologen) als Gutachter tätig werden. Auch sollte der Frage nachgegangen werden, ob *dem Gericht übergebene Unterlagen* (Gutachten) nicht eine hinreichende Grundlage bilden sollten, um den Gutachter gegen spätere ungerechtfertigte Ansprüche (Regreßansprüche) zu schützen. Wissenschaftlichen und urheberrechtlichen Interessen des Gutachters an der Bewahrung von gutachterlichen Erhebungen kann auch bei weitgehender Anonymisierung der verbleibenden Unterlagen Rechnung getragen werden.

Ich halte eine Regelung der Aufbewahrungsfristen beim Gutachter nach Erstattung des Gutachtens im Gesetz selbst für geboten.

4.2.4 Ehescheidungsverbundurteile

Als einen weiteren Bereich der Zivilprozeßordnung, der datenschutzrechtlicher Überprüfung bedarf, habe ich bereits in meinem Elften Tätigkeitsbericht (S. 21) die sogenannten Ehescheidungsverbundurteile genannt, in denen neben dem Ausspruch der Scheidung z. B. — als Folgesachen — gleichzeitig über den Umgang eines Elternteils mit dem ehelichen Kind oder über die Zahlung eines Zugewinnausgleichs entschieden wird. In der Diskussion mit dem Bundesminister der Justiz sind zwei zu unterscheidende Fragenkreise deutlich geworden:

a) Vorlage von Ehescheidungsverbundurteilen bei verschiedenen nicht am Verfahren beteiligten Dritten, z. B. bei Behörden wie der Meldebehörde, dem Standesamt (bei Wiederheirat), dem Finanzamt oder beim Arbeitgeber.

   Hier kann sich der Bürger angesichts der Zusammenfassung mehrerer Entscheidungen und der dazugehörigen Gründe in einem Urteil nicht selten gezwungen sehen, entgegen seinem Willen dieses gesamte Urteil vorzulegen, obwohl es im Einzelfall z. B. nur auf den Ausspruch über die Ehescheidung ankommt.

b) Übergabe von Ehescheidungsverbundurteilen an den Gerichtsvollzieher zum Zwecke der Zwangsvollstreckung wegen darin enthaltener vermögensrechtlicher Entscheidungen (z. B. Unterhalt, Zugewinnausgleich).

   Dabei ist davon auszugehen, daß der Gerichtsvollzieher keine Kenntnis über in dem Urteil enthaltene andere Entscheidungen — wie z. B. über das Sorgerecht für ein eheliches Kind — benötigt.

In der noch andauernden Diskussion, in die ich auch die Landesbeauftragten für den Datenschutz einbezogen habe, beginnt sich eine Lösung — zunächst jedenfalls für die erstgenannte Fallgruppe — abzuzeichnen, über die ich in meinem nächsten Tätigkeitsbericht hoffe berichten zu können.

4.3 Zentrales Handelsregister

In meinem Elften Tätigkeitsbericht (S. 22) habe ich Bedenken gegen die Zulässigkeit eines privaten zentralen Handelsregisters erhoben und dargelegt, daß § 9 des Handelsgesetzbuches (HGB), auf den sich der das Vorhaben betreibende Wirtschaftsinformationsdienst beruft, hierfür nicht als Rechtsgrundlage herangezogen werden kann.

Im Rahmen eines gerichtlichen Verfahrens gegen die Zurückweisung des Antrags des Wirtschaftsinformationsdienstes, ihm die Mikroverfilmung und elektronische Speicherung der Eintragungen des Handelsregisters zu gestatten, lag die Sache inzwischen dem Bundesgerichtshof zur Entscheidung vor. Dieser hat in seinem Beschluß vom 12. Juli 1989 (NJW 1989 S. 2818ff.) entschieden, daß § 9 HGB *kein* Recht auf Gestattung der Mikroverfilmung des gesamten Bestandes des Handelsregisters gibt, um sie als eine Datei in Konkurrenz zum Handelsregister gewerblich zu verwerten.

Diese Entscheidung bestätigt meine Auffassung. Dies gilt namentlich auch für die Gründe des Beschlusses, in denen dargelegt wird, der Wirtschaftsinformationsdienst begehre „etwas wesensmäßig anderes" als „Einsicht" in das Handelsregister; sein Anliegen gehe „über eine Einsicht in das Register weit hinaus" und werde „vom Recht auf Einsicht in § 9 Abs. 1 HGB nicht gedeckt".

Der Bundesgerichtshof führt in seinem Beschluß weiterhin aus, daß sich anderes auch nicht aus der — von mir im Elften Tätigkeitsbericht ebenfalls angesprochenen — Richtlinie des Rates der Europäischen Gemeinschaften (Amtsblatt der EG vom 14. März 1968 Nr. L 65 Seite 8ff.) ergebe, wonach vollständige oder auszugsweise Abschriften der in einem Handels- oder Gesellschaftsregister verzeichneten oder hinterlegten Urkunden oder Angaben auf schriftliches Verlangen zuzusenden sind. Demgemäß sah der Bundesgerichtshof entgegen dem Antrag des Wirtschaftsinformationsdienstes davon ab, die Sache dem Europäischen Gerichtshof vorzulegen. Ich vermag in der genannten Richtlinie des Rates der Europäischen Gemeinschaften ebenfalls keine Rechtsgrundlage für das Anliegen des Wirtschaftsinformationsdienstes zu erkennen. Derzeit wird die Angelegenheit nach einer Schriftlichen Anfrage einer Abgeordneten des Europäischen Parlaments zwischen der Kommission der Europäischen Gemeinschaften und der Bundesregierung erörtert. Ich hoffe, daß es bei der getroffenen Entscheidung bleibt.

4.4 Verwaltungsgerichtsordnung

Zunehmend wird deutlich, daß nicht nur die Strafprozeßordnung und die Zivilprozeßordnung der Verbesserung unter datenschutzrechtlichen Gesichtspunkten bedürfen, sondern daß es auch Lücken und Unzulänglichkeiten in anderen Verfahrensordnungen gibt, die zu einer gesetzgeberischen Überprüfung Anlaß geben:

Eine Petentin, die in einem Verwaltungsrechtsstreit gegen ein öffentliches Vorhaben zu klagen beabsichtigte, hat mir ihre Befürchtungen mitgeteilt, daß persönliche — insbesondere gesundheitliche — Gründe, die sie zur Begründung der Klagebefugnis vorzutragen hätte, einer größeren Zahl von weiteren Klägern zugänglich würden. Die Petentin ging hierbei offensichtlich von der Wahrscheinlichkeit eines Verbundes von „Verfahren über den gleichen Gegenstand" im Sinne des § 93 Verwaltungsgerichtsordnung (VwGO) sowie von dem Akteneinsichtsrecht der Beteiligten — bzw. Recht, sich Ausfertigungen erteilen zu lassen — nach § 100 Abs. 1 und 2 VwGO aus.

Die Verfolgung eines gleichen oder ähnlichen Anliegens durch eine Vielzahl von Klägern erfordert sicher nicht, daß jeder Kläger von jedem anderen Kläger erfährt, welche persönlichen und insbesondere gesundheitlichen Gründe die jeweilige Klagebefugnis ergeben könnten.

Der Bundesminister der Justiz, den ich zu dieser Problematik um Stellungnahme gebeten habe, hat Zweifel geäußert, ob überhaupt eine Verbindung der Verfahren nach § 93 VwGO in Betracht komme, wenn es um „die verschiedensten Gesundheitsschäden" verschiedener Bürger geht. Eine Auslegung auch des § 100 Abs. 1 und 2 VwGO „im Lichte des Volkszählungsurteils des Bundesverfassungsgerichts" dürfte entgegenstehen, daß jeder Kläger von einem anderen Kläger die Begründung der Klagebefugnis erfahre. Außerdem biete sich an, den Rechtsgedanken des § 99 Abs. 1 Satz 2 VwGO heranzuziehen. Danach kann eine Behörde die Vorlage von Urkunden und Akten und die Erteilung der Auskunft gegenüber einem Verwaltungsgericht u. a. dann verweigern, „wenn die Vorgänge nach einem Gesetz oder ihrem Wesen nach geheimgehalten werden müssen". Namentlich bei beamtenrechtlichen Konkurrentenklagen und gewerberechtlichen Streitigkeiten mit Konkurrentenbeteiligung hätten es die Verwaltungsgerichte — so führt der Bundesminister der Justiz aus — durch eine restriktive Akteneinsichtspraxis verstanden, die besonders schützenswerten Personal- und Betriebsdaten auch anderen Prozeßbeteiligten gegenüber geheimzuhalten.

Ich begrüße die Zielrichtung der Überlegungen des Bundesministers der Justiz, auch im verwaltungsgerichtlichen Verfahren einer Beeinträchtigung schutzwürdiger Belange der Betroffenen in angemessener Weise entgegenzuwirken. Die genannten Gesichtspunkte mögen hierfür übergangsweise eine gewisse Orientierung bieten; auf Dauer halte ich aber eine normenklare Regelung für unerläßlich. Dies gilt um so mehr, als der zitierte § 99 VwGO eine Vorschrift zum Schutze öffentlicher Interessen ist, als Gegenstück eine Vorschrift zum Schutze des informationellen Selbstbestimmungsrechts des einzelnen Bürgers aber fehlt. Einen erfreulichen Ansatz sehe ich in der Mitteilung des Bundesministers der Justiz, daß in seinem Hause für die Bereiche der Zivilprozeßordnung, der Freiwilligen Gerichtsbarkeit (FGG), der Verwaltungsgerichtsordnung und der Finanzgerichtsordnung geprüft werde, ob und inwieweit das Akteneinsichtsrecht einer Überarbeitung bedarf. Ich hoffe, daß mit dieser Überprüfung bald auch eine breitere Diskussionsbasis für mein Anliegen geschaffen wird.

4.5 Anwaltliche Beratungshilfe

Nach § 49a der Bundesrechtsanwaltsordnung (BRAO) ist jeder Rechtsanwalt verpflichtet, Beratungshilfe zu leisten. Nach einer solchen Tätigkeit kann er von der Landeskasse Geschäftsbesorgungs- oder Besprechungsgebühren verlangen (§ 132 Abs. 2 und 3 i. V. m. § 118 Bundesrechtsanwaltsgebührenordnung — BRAGO). Die den Ansatz der Gebühr rechtfertigenden Tatsachen hat er glaubhaft zu machen (§ 133 BRAGO i. V. m. § 128 Abs. 1 Satz 2 BRAGO, § 104 Abs. 2 und § 294 ZPO).

Bürger haben in Eingaben die Frage aufgeworfen, ob es zur Glaubhaftmachung der den Ansatz der Gebühr rechtfertigenden Tatsachen erforderlich ist, auch personenbezogene Daten des Beratenen zu offenbaren. Ich habe dies gegenüber dem Bundesminister der Justiz grundsätzlich verneint, aber für den Fall, daß es zur Glaubhaftmachung nach Lage des Einzelfalles wirklich einer Vorlage von Schriftstücken bedarf,

empfohlen zu prüfen, ob nicht — wie bei einer Weitergabe von gerichtlichen Entscheidungen an Nicht-Verfahrensbeteiligte (vgl. hierzu 9. TB S. 20) — eine anonymisierte Fassung ausreicht. In diesem Zusammenhange habe ich auch zu prüfen angeregt, ob — in Abänderung der zitierten Rechtsvorschriften — nicht an die Stelle der Glaubhaftmachung die anwaltliche Versicherung (als die eines Organs der Rechtspflege) treten sollte.

Nach Erörterung mit den Landesjustizverwaltungen hat der Bundesminister der Justiz geantwortet, er gehe in Übereinstimmung mit diesen davon aus, daß das geltende Recht in ausreichendem Umfange den Belangen des Datenschutzes und der Pflicht des Rechtsanwalts zur Verschwiegenheit Rechnung trage. Er hat ausdrücklich meine Auffassung bestätigt, daß auch dann, wenn im Einzelfall die Vorlage von Schriftstücken ausnahmsweise erforderlich ist, regelmäßig eine anonymisierte Fassung ausreicht. Ich bewerte diese Antwort als einen weitgehenden Erfolg meiner Bemühungen und habe die Landesbeauftragten für den Datenschutz gebeten, sich gegenüber der Justizverwaltung ihres Landes für eine entsprechende Praxis einzusetzen.

5 Finanzwesen

5.1 Bereichsspezifische Datenschutzvorschriften für die Finanzverwaltung

Im Elften Tätigkeitsbericht (S. 88f.) habe ich von dem Gesetzentwurf des Bundesministers der Finanzen über bereichsspezifische Datenschutzvorschriften im Anwendungsbereich der Abgabenordnung berichtet. In Abstimmung mit den Landesbeauftragten für den Datenschutz habe ich gegenüber dem Bundesminister der Finanzen inzwischen eingehend hierzu Stellung genommen. Angesichts vielfältiger Abweichungen der Regelungen des Entwurfs gegenüber dem geltenden Datenschutzrecht habe ich insbesondere kritisiert, daß der Entwurf hinter dem geltenden allgemeinen Datenschutzrecht des Bundes und der Länder deutlich zurückbleibt.

Der Bundesminister der Finanzen hat mir nunmehr mitgeteilt, nach Erörterung der ihm vorliegenden Stellungnahmen sei zwischen den Vertretern der obersten Finanzbehörden des Bundes und der Länder Übereinstimmung erzielt worden, das bisherige Konzept *ausschließlicher* bereichsspezifischer Datenschutzvorschriften im Regelungsbereich der Abgabenordnung nicht weiter zu verfolgen. Man halte es aber nach wie vor für unabdingbar, zur Sicherstellung eines *bundeseinheitlichen Datenschutzrechts im Besteuerungsverfahren* gesetzlich anzuordnen, daß sich der Datenschutz insoweit nach einheitlichen Vorschriften richtet. Dies solle dadurch erreicht werden, daß — voraussichtlich durch einen entsprechenden Hinweis in der Abgabenordnung — die Geltung des Bundesdatenschutzgesetzes auch für die *Landes*finanzbehörden vorgeschrieben werde.

Diese Entscheidung ist insofern ein Erfolg für den Datenschutz, als sie meinem Anliegen entspricht, die Einführung ausschließlicher und *unzureichender* bereichsspezifischer Datenschutzvorschriften zu verhindern. Wenn der Bundesminister der Finanzen weiterhin erwägt, für das Besteuerungsverfahren bundeseinheitlich die Geltung des Bundesdatenschutzgesetzes vorzusehen, so kann ich dieses Vorhaben nur unterstützen.

5.2 Steuerdaten-Abruf-Verordnung

Bereits im Zehnten und Elften Tätigkeitsbericht (S. 25f. bzw. S. 23f.) habe ich mich mit Fragen auseinandergesetzt, die sich bei der gemäß § 30 Abs. 6 Satz 2 bis 4 Abgabenordnung derzeit erarbeiteten „Verordnung über den automatisierten Abruf von Steuerdaten des Bundesamts für Finanzen, der Finanzämter und Gemeinden (Steuerdaten-Abruf-Verordnung — StDAV)" ergeben haben. Im Berichtsjahr konnte das Vorhaben aus datenschutzrechtlicher Sicht entscheidend vorangebracht werden.

Nach eingehender Erörterung mit dem Bundesminister der Finanzen habe ich mich davon überzeugen können, daß entgegen meiner grundsätzlichen Überlegung im Elften Tätigkeitsbericht (S. 23) eine Aufzeichnung *sämtlicher* Datenabrufe durch Abrufberechtigte aus anderen als für die Sachbearbeitung zuständigen Organisationseinheiten der speichernden Behörde *nicht* erforderlich ist, um eine ausreichende Kontrolle zu gewährleisten. Die arbeitsteilige Bearbeitung der Vorgänge bei verschiedenen Stellen eines Finanzamtes mit jeweils eigenen Aufgaben (z. B. Veranlagungsstelle, aber auch Finanzkasse) führt dazu, daß andere als die sachbearbeitenden Organisationseinheiten in einer *Vielzahl* von Fällen *befugt* auf die Daten der sachbearbeitenden Organisationseinheit zugreifen. Aus der Sicht des Schutzes dieser Daten vor mißbräuchlichem Abruf stünde eine Protokollierung aller dieser Abrufe außer Verhältnis zu einer möglichen Gefährdung durch *unbefugte* Abrufe. Ich halte es daher für angemessen, als Vorsorgemaßnahme für eine Kontrolle der Datenabrufe — wie im Entwurf vorgesehen — deren programmgesteuerte Aufzeichnung in Form eines *zufallsbestimmten Stichprobenverfahrens* vorzuschreiben. Dabei sehe ich auch keinen grundsätzlichen Unterschied darin, ob es um Datenabrufe von für die Sachbearbeitung nicht zuständigen Organisationseinheiten *innerhalb* der speichernden Behörde geht oder um Abrufe aus *anderen Finanzbehörden,* denen aufgrund landesrechtlicher Regelung nach § 17 Abs. 2 Satz 3 oder nach § 17 Abs. 3 Satz 1 des Finanzverwaltungsgesetzes die *zentrale* Erledigung bestimmter Aufgaben (z. B. Veranlagung, Erhebung der Steuern) übertragen ist.

Wesentlich ist allerdings für mich — und insofern habe ich eine Festlegung im Entwurf erreicht —, daß sich die Häufigkeit der Stichproben entsprechend dem Schutzbedürfnis der Daten insbesondere nach dem Umfang der „Zugriffsbefähigung" der abrufenden Organisationseinheit im Verhältnis zur Anzahl der in einem Zeitraum zu bearbeitenden Fälle richtet. Je umfassender dabei die Zugriffsbefähigung ist (z. B. bei Betriebsprüfungsstellen in der speichernden Behörde oder in einer zentral beauftragten Finanzbehörde), desto größer ist das Schutzbedürfnis. Dann kann es erforderlich sein, über den für die Stichprobe

vorgesehenen Mindestsatz von 5 % der Abrufe erheblich hinauszugehen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte — wie im Elften Tätigkeitsbericht (S. 23f.) berichtet — Bedenken dagegen erhoben, daß im Entwurf der Steuerdaten-Abruf-Verordnung für besonders ermächtigte Amtsträger der obersten Finanzbehörden und der Oberfinanzdirektionen die Möglichkeit zum Abruf von Daten der Finanzämter vorgesehen werden soll. Für Amtsträger der *obersten Finanzbehörden* hat der Bundesminister der Finanzen auf die Möglichkeit einer Datenabrufberechtigung nahezu vollständig verzichtet. Als einzige Ausnahme hält der Bundesminister der Finanzen daran fest, Amtsträgern oberster Landesfinanzbehörden, die mit der Erstellung und Wartung von Programmen zur Verarbeitung von Daten im Sinne der Steuerdaten-Abruf-Verordnung befaßt sind, die Möglichkeit einer Abrufberechtigung zur Beseitigung von Fehlern oder zur Kontrolle der bestimmungsgemäßen Arbeitsweise der Programme einzuräumen, eine Regelung, die landesrechtlichen Organisationsentscheidungen Rechnung tragen soll.

Wegen der im Entwurf vorgesehenen Abrufmöglichkeiten für Amtsträger von *Oberfinanzdirektionen* haben sich Mitarbeiter meiner Dienststelle gemeinsam mit Vertretern der Datenschutzkommission Rheinland-Pfalz und des Hessischen Datenschutzbeauftragten bei der Oberfinanzdirektion Koblenz über die praktische Bedeutung und die sachliche Notwendigkeit des Abrufs von Daten der Finanzämter durch Oberfinanzdirektionen unterrichtet. Aufgrund der dort vermittelten Erkenntnisse kann ich mich nicht dem Erfordernis verschließen, für bestimmte Fallgruppen — z. B. Entscheidungen über Stundungsanträge, für die u. a. der aktuelle Kontenstand beim Finanzamt wesentlich ist — die Möglichkeit zuzulassen, besonders ermächtigten Amtsträgern der Oberfinanzdirektionen die Berechtigung zu Datenabrufen zu geben. Entscheidend ist für mich dabei aber, daß diese Fallgruppen im einzelnen präzise im Entwurf umschrieben und eingegrenzt werden. Der Bundesminister der Finanzen stimmt derzeit auf der Grundlage eines von mir vorgelegten Vorschlags für eine Festlegung dieser Fallgruppen entsprechende Regelungen mit den obersten Landesfinanzbehörden ab.

Angesichts des Bearbeitungsstandes des Entwurfs gehe ich davon aus, daß die aus datenschutzrechtlicher Sicht wichtige Steuerdaten-Abruf-Verordnung in absehbarer Zeit erlassen werden kann.

5.3 Abschriften von Urkunden an Finanzbehörden

Die zuständigen Finanzbehörden benötigen für die ordnungsgemäße Durchführung der Besteuerung die jeweils relevanten personenbezogenen Daten des Steuerpflichtigen und ggf. auch dritter Personen. Wenn Gerichte, Notare und sonstige Urkundsbeamten im Rahmen ihrer Anzeigepflicht nach § 34 Erbschaftsteuer- und Schenkungsteuergesetz (ErbStG) gemäß § 12 Abs. 1 und 5 Erbschaftsteuer-Durchführungsverordnung (ErbStDV) vor allem beglaubigte Abschriften der eröffneten Verfügungen von Todes wegen an das zuständige Finanzamt übersenden, werden dabei allerdings vielfach — zum Teil recht persönliche — Erklärungen mit personenbezogenen Daten mitgeteilt, die steuerrechtlich ohne Bedeutung sind (z. B. Erläuterungen von Motiven des Erblassers; Ratschläge, Ermahnungen an die Erben). Gleiches gilt z. B. auch für die Übersendung beglaubigter Abschriften von Urkunden über Schenkungen (vgl. § 13 Abs. 2 ErbStDV). Ebenso werden dem zuständigen Finanzamt teilweise nicht benötigte Daten übermittelt, wenn Gerichte, Behörden und Notare diesem gemäß § 18 Abs. 1 Grunderwerbsteuergesetz (GrEStG) Abschriften der Urkunden über Rechtsvorgänge, die ein Grundstuck betreffen, wie z. B. Abschriften von Grundstückskaufverträgen, übersenden.

Ich habe den Bundesminister der Finanzen gebeten zu prüfen, ob Gerichte, Notare und sonstige Urkundspersonen nicht *anstelle* der Übersendung beglaubigter Abschriften nach § 12 Abs. 1 und 5 sowie nach § 13 Abs. 2 ErbStDV eine schriftliche Erklärung anhand eines Formulars abgeben können, das ähnlich wie der Vordruck „Antrag auf Lohnsteuer-Jahresausgleich/Einkommensteuererklärung" die in der Regel steuerlich maßgeblichen Fragen enthält; möglicherweise ließe sich der nach Muster 5 zu § 12 ErbStDV ohnehin auszufüllende Vordruck entsprechend erweitern. Bei Zweifeln und ergänzenden Fragen des Finanzamts könnten, soweit erforderlich, beglaubigte Auszüge von eröffneten Verfügungen von Todes wegen oder von Schenkungsurkunden vorgelegt werden, in denen steuerrechtlich unerhebliche Erklärungen geschwärzt oder überhaupt nicht mehr enthalten sind. Soweit es um die Übersendung von Abschriften von Urkunden nach § 18 Abs. 1 GrEStG geht, habe ich ebenfalls den Vorschlag einer schriftlichen Erklärung anhand eines Formulars zu erwägen gegeben; möglicherweise könnte der nach dieser Vorschrift amtlich vorgeschriebene Vordruck für die „Anzeige" des Rechtsvorgangs an das zuständige Finanzamt entsprechend erweitert werden. Bei Nachfrage durch das Finanzamt könnte er wiederum durch die Vorlage auszugsweiser Abschriften ergänzt werden, die steuerlich unerhebliche Erklärungen nicht enthalten.

Eine Antwort des Bundesministers der Finanzen auf mein erst gegen Ende des Berichtszeitraums übersandtes Schreiben steht noch aus.

5.4 Abfertigung von Übersiedlungsgut

Die Bundeszollverwaltung fertigt bei der Einreise von *Aussiedlern* aus Osteuropa deren Umzugsgut mit einem zweiseitigen Formular „zum freien Verkehr" ab. Dabei werden den Aussiedlern regelmäßig zeitlich begrenzte Verfügungsbeschränkungen über ihr Umzugsgut (Übersiedlungsgut) auferlegt. Blatt 1 des Formulars verbleibt für zehn Jahre als Beleg in einer Sammlung der abfertigenden Zollstelle; Blatt 2 erhält der Aussiedler und Blatt 3 wird dem zuständigen Hauptzollamt zu einer Sammlung für die Überwachung der Verwendung des Übersiedlungsgutes übersandt.

Dieses Verfahren stützt sich auf die Verordnung Nr. 918/83 des Rates der Europäischen Gemeinschaften über das gemeinschaftliche System der Zollbefreiungen (Amtsblatt der EG vom 23. April 1983 Nr. L 105 Seite 1ff.). Hiernach bleibt das Übersiedlungsgut zwar unter bestimmten Voraussetzungen frei von Eingangsabgaben; es unterliegt jedoch grundsätzlich einer *zwölfmonatigen Zweckbindung*, d. h. es darf während dieser Zeit weder verliehen, verpfändet, vermietet, veräußert oder sonst überlassen werden. Ob diese Regelung sinnvoll ist und ihre Einhaltung überhaupt überwacht werden kann, ist von mir nicht zu beurteilen.

Durch eine Eingabe bin ich darauf hingewiesen worden, daß das Übersiedlungsgut der Aussiedler aus Osteuropa vielfach nur von geringem Wert ist und neben persönlichen Erinnerungsstücken oft z. B. nur gebrauchtes Bettzeug und veraltetes Küchengerät umfaßt. Ich bin an den Bundesminister der Finanzen mit der Bitte herangetreten, insoweit die Erforderlichkeit des Abfertigungsverfahrens in der vorgenannten Form einschließlich der bei der Zollstelle und beim Hauptzollamt entstehenden Sammlungen von personenbezogenen Daten von Aussiedlern unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit zu prüfen. Dies gilt besonders deshalb, weil — wie dargelegt — einerseits Blatt 1 des Formulars zehn Jahre bei der Zollstelle aufbewahrt wird, während andererseits in der Verordnung Nr. 918/83 des Rates der Europäischen Gemeinschaften nur eine zwölfmonatige Zweckbindung des Übersiedlungsgutes vorgesehen ist.

In seiner Antwort hat der Bundesminister der Finanzen auf die vorgenannten Regelungen der Verordnung Nr. 918/83 des Rates der Europäischen Gemeinschaften und die darin festgelegte grundsätzliche zwölfmonatige Zweckbindung des Übersiedlungsgutes verwiesen. Er hat aber auch mitgeteilt, daß die Verordnung bei Vorliegen außergewöhnlicher politischer Umstände Abweichungen von der zwölfmonatigen Zweckbindung des Übersiedlungsgutes zuläßt; bei Aussiedlern aus Osteuropa sieht er die Voraussetzungen dafür als gegeben an. Der Bundesminister der Finanzen hat deshalb die Zollstellen aufgefordert, bei Übersiedlungsgut mit geringem Wert auf die förmliche Zollanmeldung zu verzichten, soweit die Merkmale und Umstände offensichtlich sind und — wie hier — von der Festsetzung der Bindungsfrist abgesehen werden kann; der Zollantrag ist dann mündlich zu stellen (§ 18 Abs. 1 Allgemeine Zollordnung). Die Folge ist, daß Belege nicht anfallen und nicht erforderliche Datensammlungen gar nicht erst entstehen.

Die auf meine Initiative erreichte Regelung bedeutet nicht nur einen beachtenswerten Fortschritt für den Datenschutz, sondern auch eine Verwaltungsvereinfachung, deren Bedeutung durch das starke Ansteigen der Aussiedlerzahlen im Berichtsjahr erheblich gewachsen ist.

6 Personalwesen

6.1 Bundesanstalt für das Straßenwesen

Im Berichtsjahr haben meine Mitarbeiter eine Kontrolle bei der Bundesanstalt für das Straßenwesen (BASt) durchgeführt. Die Kontrolle führte im wesentlichen zu folgenden Feststellungen und Empfehlungen:

— *Telefondatenverarbeitung*

Die Behörde hat noch während der Kontrolle eine meinen Anregungen und den geltenden Dienstanschlußvorschriften entsprechende Änderung des Verfahrens der Datenerhebung und -verarbeitung sowie der Aufbewahrungsdauer von Gesprächsnachweislisten für Privatgespräche zugesagt.

— *Personaldatei (PERSDAT)*

Es wurde festgestellt, daß im Rahmen des automatisierten Personaldatenverarbeitungssystems freie Abfragen der gespeicherten Daten und frei erstellbare Sortierungen und Auswertungen des Datenbestandes in geringer Anzahl vorgenommen wurden, obwohl dies in der zwischen Dienststelle und Gesamtpersonalrat bestehenden Vereinbarung über die automatische Verarbeitung personenbezogener Daten im Bereich der Personalverwaltung nicht vorgesehen ist; diese Vereinbarung enthält vielmehr als Anlage den Datenkatalog und eine Aufstellung aller zulässigen Auswertungen.

Ich habe empfohlen, die bisher in der Vereinbarung nicht erfaßten, aber für erforderlich gehaltenen „freien Abfragen" inhaltlich festzulegen, mit der Personalvertretung abzustimmen und in den Anhang der Dienstvereinbarung aufzunehmen. Ein solches Verfahren trägt den schutzwürdigen Belangen der Mitarbeiter besonders Rechnung.

— *Beihilfesachbearbeitung*

Beihilfevorgänge werden bei der BASt von Mitarbeitern des Personalbüros bearbeitet, in Zweifelsfällen dem Leiter des Personalbüros vorgelegt und nach Bearbeitung jeweils der Vorprüfstelle des BMV zugeleitet, die einen Prüfungsvermerk anbringt.

Ich habe entsprechend meiner bereits früher (vgl. 10. TB S.27; 9. TB S. 22f.) vertretenen Auffassung gefordert, die Beihilfestelle organisatorisch und personell von der Personalbearbeitung zu trennen und empfohlen, in Zukunft nicht mehr alle Beihilfeanträge an die Vorprüfungsstelle des BMV zu übersenden, zumal der Bundesrechnungshof eine Stichprobenprüfung von Beihilfeanträgen als ausreichend ansieht.

6.2 Kontakte zwischen Personalvertretungen und dem Bundesbeauftragten für den Datenschutz

Bereits in meinem Zehnten Tätigkeitsbericht habe ich mich mit der Frage der Zulässigkeit unmittelbarer Kontakte zwischen Personalvertretungen und meiner Dienststelle beschäftigt (s. 10. TB S. 31).

Ein im Berichtsjahr vom Wissenschaftlichen Dienst des Deutschen Bundestages erstelltes Rechtsgutachten bestätigt in weitem Umfang meine Auffassung. Danach kann ich mich jederzeit unmittelbar an jede Personalvertretung wenden. Den Personalvertretungen steht nach der im Gutachten vertretenen Auffassung zwar ein Recht, den Bundesbeauftragten nach § 21 BDSG anzurufen, nicht zu; das heißt aber nicht, daß damit jede Kontaktaufnahme einer Personalvertretung mit mir ausgeschlossen wäre. Ganz im Gegenteil. Stellung, Aufgaben und Befugnisse des Bundesbeauftragten bedingen, wie das Gutachten ausdrücklich betont, daß auch jede Personalvertretung ohne vorherige Einschaltung der Dienststelle Fragen und Informationen — etwa „über Gefahrenlagen und Mißstände sowie Verbesserungsvorschläge" — an mich herantragen oder meine Beratung suchen kann. Unabhängig hiervon kann sich natürlich jedes einzelne Personalratsmitglied wie jede andere natürliche Person als persönlich Betroffener oder als ermächtigter Vertreter eines Mitarbeiters einer Bundesbehörde an mich wenden. Um künftig Probleme in diesem Bereich zu vermeiden, empfehle ich nachdrücklich, im Entwurf eines Gesetzes zur Änderung des Bundespersonalvertretungsgesetzes eine entsprechende Klarstellung zu treffen.

6.3 Telefondatenverarbeitung

Auch im zurückliegenden Jahr hatte ich mich ausführlich mit Fragen der Telefondatenverarbeitung zu beschäftigen.

Eine Petenteneingabe betraf die Datenverarbeitung im Zusammenhang mit privaten Telefongesprächen bei der *Fachhochschule des Bundes für öffentliche Verwaltung, Fachbereich Flugsicherung und Wetterdienst.* Nach längeren Erörterungen konnte ich in diesem Fall eine Reihe datenschutzrechtlicher Unzulänglichkeiten abstellen und eine Lösung erreichen, die in vorbildlicher Weise die Anforderungen des Datenschutzes berücksichtigt. Ich erkenne insbesondere an, daß auf meine Anregungen hin in Zusammenarbeit mit der Herstellerfirma die Systemsoftware trotz der hiermit verbundenen Kosten entsprechend geändert und damit der Verzicht auf die Speicherung der letzten Ziffern der Zielnummer technisch ermöglicht wurde. Ich sehe damit meine Auffassung bestätigt, daß eine derartige zur Gewährleistung des Datenschutzes erforderliche Softwareänderung bei gutem Willen ohne große Schwierigkeiten möglich ist.

Leider waren meine Bemühungen um eine datenschutzgerechte Telefondatenverarbeitung nicht überall erfolgreich. So hatte ich bereits 1988 die *Bundesanstalt für Flugsicherung* auf Unzulänglichkeiten bei der dort praktizierten Speicherung und Verarbeitung von Telefondaten aufmerksam gemacht. Trotz mehrerer Aufforderungen und zugesagter Antwort im Berichtsjahr hat sie auf meine datenschutzrechtlichen Empfehlungen bis zum Redaktionsschluß nicht reagiert.

Auch die *Deutsche Genossenschaftsbank (DG-Bank)* hat sich bis Redaktionsschluß nicht bereit erklärt, das derzeit praktizierte Telefondatenerfassungsverfahren datenschutzgerechter zu gestalten.

In beiden Fällen sehe ich einen bedauerlichen Mangel an Aufgeschlossenheit für den Datenschutz und an Kooperationsbereitschaft. Ich werde die Angelegenheiten weiterverfolgen.

6.4 Dezentrale Leistungs- und Kostenrechnung bei der Deutschen Bundespost (DELKOS)

Die Deutsche Bundespost hat die Konzeption für ein computergestütztes System einer dezentralen Leistungs- und Kostenrechnung im Jahrbuch der Deutschen Bundespost 1986 veröffentlicht.

Anfang 1988 kam es zwischen der Deutschen Bundespost und deren Hauptpersonalrat zu einer Auseinandersetzung über die Einführung dieses Verfahrens. Der Hauptpersonalrat stimmte der Einführung des Systems nicht zu. Die daraufhin eingeschaltete Einigungsstelle beschloß, der Einführung des Systems DELKOS mit der Maßgabe zuzustimmen, daß der Bundesbeauftragte für den Datenschutz zur Stellungnahme aufzufordern und zwischen dem BMPT und dem Hauptpersonalrat über die weitere Beteiligung der Personalvertretungen eine Dienstvereinbarung abzuschließen sei.

In mehreren Gesprächen, an denen Vertreter des BMPT, des Hauptpersonalrats und ich beteiligt waren, wurden die Konzeption von DELKOS und die damit zusammenhängenden datenschutzrechtlichen Probleme ausführlich erörtert. In meiner abschließenden Bewertung bin ich im wesentlichen zu folgenden Feststellungen und Empfehlungen gekommen:

Die Einführung von DELKOS dient der Bereitstellung entscheidungsrelevanter Kosten- und Erlösdaten sowie der Kontrolle der Wirtschaftlichkeit auf allen Stufen des Unternehmens. Es sind drei Dateien mit Personaldaten vorgesehen: eine Personalstammdatei, eine Ausfalldatei zur Ermittlung der Ausfallzeiten sowie eine Zulagen- und Entschädigungsdatei. Die in diesen Dateien enthaltenen Daten werden so lange personenbezogen erfaßt und gespeichert, bis ein geplantes automatisiertes Personaldatenverwaltungssystem in Betrieb geht, das die von DELKOS benötigten aufbereiteten Daten zur Verfügung stellen kann.

Ich habe empfohlen, die in den drei Dateien zu verarbeitenden Datenarten in einer Dienstvereinbarung sowie einer Dienstanweisung festzulegen.

Es besteht Übereinstimmung, daß eine personenbezogene Auswertung der in DELKOS erfaßten Daten für die Erfüllung des angestrebten Zwecks nicht erforderlich ist und deshalb auch nicht erfolgen darf. Darum muß eine personenbezogene Auswertung generell und zwar auch für die Fälle ausgeschlossen werden, in denen nach Aufbereitung der Datenbestände für

DELKOS der Personenbezug nicht vollständig aufgehoben ist. Eine mögliche Nutzung von DELKOS zur Verhaltens- und Leistungskontrolle sollte in Dienstvereinbarung und Dienstanweisung ausdrücklich ausgeschlossen werden.

In Dienstanweisung und Dienstvereinbarung sollten weiterhin angemessene Löschungsfristen für die erhobenen personenbezogenen Daten sowie die Vernichtung der im Rahmen von DELKOS verwendeten Belege festgelegt werden.

Soweit vorgesehen ist, APC als Arbeitshilfen für DELKOS-Sachbearbeiter zur Verfügung zu stellen, um Rechenarbeiten zu erledigen, habe ich angemessene technische und organisatorische Schutzmaßnahmen empfohlen: Technisch ist die Einrichtung von Verbindungen zwischen den APC und den DELKOS-Terminals auszuschließen und sicherzustellen, daß mit den APC auch auf andere Weise nicht auf DELKOS-Daten zugegriffen wird oder Eingaben in das System vorgenommen werden. In organisatorischer Hinsicht sollte das Eingabeverfahren für personenbezogene Daten so gestaltet werden, daß eine — unzulässige — Nutzung eines APC keine Vorteile für den Benutzer zur Folge hätte. Zusätzlich habe ich neben einer eindeutigen Weisung, auf diesen APC keine personenbezogenen Daten zu verarbeiten, Belehrungen und Kontrollen in angemessenem Umfang für erforderlich erklärt.

Die Verhandlungen zwischen dem BMPT und dem Hauptpersonalrat über den Abschluß einer Dienstvereinbarung werden voraussichtlich Anfang 1990 zum Abschluß kommen.

6.5 Arbeitszeitüberwachung durch automatisierte Kontrollsysteme

Aufgrund einer Eingabe hatte ich während des Berichtszeitraums die Zulässigkeit eines automatisierten Kontrollsystems zu beurteilen, das der Arbeitszeitüberwachung bei gleitender Arbeitszeit diente (vgl. auch 3. TB S. 28 und S. 29 und 5. TB S. 29).

Gegen die vorgesehene stichprobenweise Auswertung der automatisierten Aufzeichnungen durch den Dienststellenleiter bestehen aus der Sicht des Datenschutzes keine Bedenken.

Ich habe ferner darauf hingewiesen, daß die im Rahmen des Kontrollverfahrens gemachten Aufzeichnungen nicht länger aufbewahrt werden dürfen, als es für die angestrebten Zwecke erforderlich ist. Dabei kommt den Fristen, die für die Aufrechnung der Arbeitszeiten vorgesehen sind (sie sollten einen Monat nicht überschreiten) besondere Bedeutung zu. Die aufgezeichneten Daten sind nach Fristablauf zu löschen.

Sollte ein Kontrollsystem über die Arbeitszeiterfassung hinaus auch noch anderen Zwecken — z. B. der Zugangssicherung und dem Nachweis des Aufenthaltes in einem gesicherten Bereich — dienen, sind für die diesen Zwecken dienenden Daten unter Sicherheitsaspekten gegebenenfalls längere Aufbewahrungsfristen festzulegen. Die Nutzung dieser Speicherungen ist dann auf Sicherheitsrevisionen und Einzelauswertungen bei Sicherheitsverstößen zu beschränken.

In meiner Stellungnahme zu dem geprüften System habe ich auch zum Ausdruck gebracht, daß Auswertungen der mit diesem Kontrollsystem gewonnenen Daten zu anderen als den jeweils festgelegten Zwekken, wie z. B. für eine Statistik, nur in anonymisierter Form, also ohne Bezug zu den einzelnen Bediensteten, zulässig sind.

6.6 Beihilfeverfahren

6.6.1 Eigene Rechtsstellung für Angehörige

— Eine von ihrem Ehemann getrennt lebende Petentin hat sich darüber beschwert, daß sie gezwungen sei, im Rahmen des Beihilfeverfahrens ihrem beihilfeberechtigten Ehemann die ärztlichen Befundunterlagen mit hochsensiblen Gesundheitsdaten zugänglich zu machen.

— In einer anderen Eingabe hat mir eine Fachärztin für Psychiatrie mitgeteilt, daß der Ehemann ihrer Patientin das über diese im Rahmen des Beihilfeverfahrens erstattete und ihm übergebene Gutachten zur Grundlage einer Scheidungsklage gemacht habe.

Diese Fälle, die noch durch weitere ergänzt werden könnten, veranlaßten mich, gegenüber dem Bundesminister des Innern eine Überarbeitung der Beihilfevorschriften anzuregen.

Nach dem geltenden Beihilferecht steht nur dem beihilfeberechtigten Angehörigen des öffentlichen Dienstes ein Anspruch auf Leistung für seine Familienangehörigen zu. Diese haben keinen selbständigen Beihilfeanspruch; sie sind vielmehr gezwungen, dem Beihilfeberechtigten die Inanspruchnahme jeder Art von beihilfefähiger Leistung durch Übermittlung der Belege zur Vorlage bei der Beihilfestelle zu offenbaren.

Die früher in der gesetzlichen Krankenversicherung geltende vergleichbare Rechtslage ist durch das Gesundheits-Reformgesetz datenschutzfreundlich geändert worden. Gemäß § 10 dieses Gesetzes sind die Angehörigen eines Kassenmitgliedes nunmehr ebenfalls Versicherte mit eigenen Leistungsansprüchen und insoweit den Kassenmitgliedern insbesondere auch im Hinblick auf die Erhebung, Verarbeitung und Löschung ihrer Daten und ihrer Auskunftsrechte gleichgestellt.

Das Bundesministerium des Innern hat meine Anregung aufgegriffen und insbesondere die Frage eines eigenen Antragsrechts auf Beihilfe für bei der Beihilfe berücksichtigungsfähige Familienangehörige in der Bund-Länder-Kommission für das Beihilferecht erörtert. Das Ergebnis war allerdings, daß die Einführung eines solchen Antragsrechts nicht möglich sei. Gestützt wird diese Entscheidung insbesondere darauf, daß aus dem Dienstverhältnis resultierende Ansprüche nur dem Beamten selbst zustehen könnten, weil die Fürsorgepflicht nach § 79 Bundesbeamtengesetz

keine eigenen Ansprüche einzelner Angehöriger gegenüber dem Dienstherrn begründe. Das Bundesministerium des Innern erwägt, meinem Anliegen „auf eng begrenzte Ausnahme- und Sondertatbestände beschränkt" durch folgende Verfahrensregelung Rechnung zu tragen: Die betreffenden Familienangehörigen leiten ihre Unterlagen direkt der Beihilfestelle zu, während der Beihilfeberechtigte im Antragsformular hierauf lediglich Bezug nimmt; ebenso werden die Unterlagen von der Beihilfestelle unmittelbar an die Betroffenen zurückgesandt.

Dieses vom Bundesministerium des Innern vorgeschlagene Verfahren — soweit überhaupt praktikabel — ist zwar ein Schritt in die richtige Richtung, wird aber den Ansprüchen des Rechts auf informationelle Selbstbestimmung der betroffenen Angehörigen noch nicht gerecht. Ich bin nicht davon überzeugt, daß die Einräumung eines eigenen Beihilfeanspruchs für Familienangehörige tatsächlich mit den hergebrachten Grundsätzen des Berufsbeamtentums unvereinbar ist. Eine solche Regelung bevorzuge ich nach wie vor. Dies auch deshalb, weil sie geeignet wäre, auch andere im Zusammenhang mit den Beihilfevorschriften auftretende datenschutzrechtliche Probleme in Bezug auf das Auskunftsrecht, die Berichtigung und Löschung gespeicherter Daten der Familienangehörigen zu lösen.

Ich werde eine dem Datenschutz entsprechende Regelung gegenüber dem Bundesministerium des Innern weiterverfolgen. Gelegenheit zu einer sachgerechten Lösung könnte die vorgesehene gesetzliche Regelung des Personalaktenrechts bieten, die auch zu weiteren erwünschten Verbesserungen des Beihilferechts im Hinblick auf den Datenschutz genutzt werden sollte.

6.6.2 Automatisiertes Beihilfeverfahren

Mehrere oberste Bundesbehörden sind im Begriff, die Beihilfebearbeitung auf automatisierte Verfahren umzustellen. So befindet sich im Auswärtigen Amt ein vom Land Baden-Württemberg übernommenes und den Belangen des Bundes angepaßtes Bildschirm-Dialogverfahren „BABSY" (Beihilfeabrechnungssystem) in der Einführungsphase; der Bundesminister der Verteidigung bereitet die Übernahme dieses Systems vor. Der BMF entwickelt ein vergleichbares Verfahren.

Während eines Informationsbesuchs im Auswärtigen Amt habe ich folgende datenschutzrechtlich relevanten Feststellungen treffen können: Das System umfaßt je eine Stammsatzdatei für Bedienstete und deren Familienangehörige, eine Belegedatei mit Daten von Beihilfeanträgen und Belegen, eine Bearbeitungsdatei nicht abgeschlossener Beihilfefälle und eine „Zugriffsdatei" mit personenbezogenen Daten der Zugriffsberechtigten. Diese Dateien werden im Rahmen eines Menüs mit zahlreichen Masken genutzt, die in einem „BABSY-Handbuch" im einzelnen beschrieben sind. Die Zugriffsberechtigungen sind streng funktionsbezogen begrenzt.

Das Auswärtige Amt hat zugesichert, daß Diagnosen nicht gespeichert werden. Dies trifft auch zu. Einige der zur korrekten Abrechnung der Beihilfe erforderlichen Daten, wie z. B. die Zahl der genehmigten psychotherapeutischen Sitzungen oder die Stärke von Brillengläsern bzw. Haftschalen, lassen aber durchaus gewisse Rückschlüsse auf gesundheitliche Beeinträchtigungen zu. Ich werde gegenüber dem Auswärtigen Amt darauf hinwirken, daß die Speicherung derartiger Daten auf das unerläßliche Maß beschränkt und die notwendigen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherung getroffen werden.

6.7 Personalwesen — Einzelfälle

Im Berichtszeitraum haben mich u. a. folgende Einzelfragen beschäftigt:

— Mit dem Inhalt von *Bewerbungs- und Personalbögen* habe ich mich bereits in der Vergangenheit mehrfach befaßt (siehe 6. TB S. 21; 3. TB S. 26). Einige Eingaben im Berichtsjahr deuten darauf hin, daß die Praxis bei der Erhebung von Personaldaten weiterhin sehr unterschiedlich ist. Ich habe bereits früher die grundsätzliche Auffassung vertreten, daß Inhalt der Bewerbungsunterlagen ausschließlich die für die Entscheidung über die Einstellung des Bewerbers erforderlichen Informationen sein sollen. Die von den Bewerbungsunterlagen zu unterscheidenden Einstellungsunterlagen dürfen auch Informationen enthalten, die z. B. für die Berechnung der Besoldung erforderlich sind. An dieser Auffassung halte ich weiter fest.

— Der auf Beurteilungsrichtlinien zurückgehende *Beurteilungsbogen der BfA* enthält u. a. Feststellungen zum Gesundheitszustand und zur äußeren Erscheinung des Beurteilten. Ich habe diese Fragen unter Aspekten des Personaldatenschutzes als unzulässig bewertet. Gesundheitszeugnisse dürfen nur unter sehr eingeschränkten Voraussetzungen in die Personalakte des Bediensteten aufgenommen werden (siehe 8. TB S. 14 f.). Da der Beurteiler darüber hinaus in der Regel medizinischer Laie sein dürfte, ist eine fachgerechte Bewertung des Gesundheitszustandes durch ihn kaum zu erwarten. Eine Beurteilung der äußeren Erscheinung ist kaum objektivierbar. Die BfA hat sich bereit erklärt, von einer Bewertung des Gesundheitszustandes in den dienstlichen Beurteilungen künftig abzusehen. Nach der äußeren Erscheinung des zu beurteilenden Mitarbeiters soll allerdings weiterhin gefragt werden. Die BfA prüft seit einiger Zeit eine Änderung der Beurteilungsrichtlinien. Ein abschließendes Ergebnis steht noch aus.

— Eine Eingabe betraf die Weitergabe von personenbezogenen Daten in einer Dienststelle des Bundesministers der Verteidigung. Anläßlich eines Beurteilungstermins wurden *Listen mit Personaldaten* aller Soldaten eines Bataillions entsprechend der Beurteilungsnote in einer Wertungsreihenfolge zusammengestellt und von dem Bataillonskommandeur allen Batteriechefs dieses Bataillons ausgehändigt. Die Batteriechefs hatten damit die Möglichkeit, Kenntnis von Personaldaten ihnen nicht unterstellter Soldaten zu nehmen. Ich habe

die Verteilung der Listen als Verletzung des Personalaktengeheimnisses gewertet. Soweit die Batteriechefs keine Dienstvorgesetzten der Soldaten waren, war die Bekanntgabe der personenbezogenen Daten zur Durchführung des Dienstverhältnisses nicht erforderlich. Der BMVg hat eingeräumt, daß die Vorgehensweise nicht den einschlägigen Weisungen auf dem Gebiet des Datenschutzes und des Beurteilungswesens entsprach. Er hat den Vorfall, bei dem es sich um einen Einzelfall handelte, zum Anlaß einer entsprechenden Unterrichtung seiner Führungskräfte genommen.

— Ein Petent hat mir mitgeteilt, er sei von seinem Vorgesetzten gefragt worden, ob er sich mit einer *datenschutzrechtlichen Beschwerde* an mich gewandt habe. Er befürchtet, daß ihm aus einer wie immer gearteten Antwort dienstliche Nachteile erwachsen könnten. Ich vertrete hierzu die Auffassung, daß eine solche Frage als unzulässige Datenerhebung anzusehen ist, weil es insoweit an der Erforderlichkeit für die Durchführung des Dienstverhältnisses fehlt. Hinzu kommt, daß gemäß § 21 BDSG jedermann das Recht hat, sich an den Bundesbeauftragten für den Datenschutz zu wenden. Es muß gewährleistet sein, daß die Inanspruchnahme dieses Rechts zu keinerlei dienstlichen Nachteilen führt.

— Bei der datenschutzrechtlichen Bewertung der *automatisierten Personalverarbeitung der Physikalisch-Technischen Bundesanstalt,* Braunschweig, habe ich Bedenken gegen die vorgesehenen freien Abfragemöglichkeiten geäußert.

Zu den datenschutzrechtlichen Risiken freier Abfragesprachen habe ich bereits in meinem Neunten Tätigkeitsbericht (S. 27) Stellung genommen und im Zehnten Tätigkeitsbericht empfohlen, in Vereinbarungen zwischen Dienststelle und Personalvertretung freie Abfragesprachen auszuschließen (10. TB S. 32). Grundsätzlich lassen sich alle Bearbeitungszwecke und die zu ihrer Umsetzung erforderlichen Arbeitsschritte der Personaldatenverarbeitung jeweils im einzelnen festlegen. In den mir bisher bekanntgewordenen Systemen automatisierter Personaldatenverarbeitung ist daher — teilweise allerdings erst auf mein Betreiben hin — auf die Einrichtung freier Abfragemöglichkeiten verzichtet worden.

Auch im Fall der Physikalisch-Technischen Bundesanstalt ließen sich keine überzeugenden Gründe für die Erforderlichkeit freier Abfragemöglichkeiten erkennen. Aus der Sicht des Datenschutzes ist zu begrüßen, daß die Bundesanstalt meine Bedenken gegen die Einräumung freier Abfragemöglichkeiten aufgegriffen und die Auswertungsverfahren nunmehr lückenlos festgelegt hat.

— Ein Petent war nach einem *Freizeitunfall* für einige Monate dienstunfähig erkrankt. Er beschwerte sich darüber, daß sein Dienstherr ohne sein Wissen Unterlagen über sein Krankheitsbild bei der Reha-Klinik angefordert hatte, um sie vom amtsärztlichen Dienst im Hinblick auf eine mögliche Polizeidienstunfähigkeit überprüfen zu lassen. Ich habe diese Verfahrensweise als Verstoß gegen das Recht auf informationelle Selbstbestimmung des Petenten gewertet. Da während der Zeit der Dienstunfähigkeit persönliche Kontakte zwischen Dienstherrn und Petenten bestanden, wäre es möglich und geboten gewesen, den Petenten von der beabsichtigten Einholung eines Befundberichtes zu unterrichten. Ich habe empfohlen, eine entsprechende Unterrichtungspflicht in die Verfahrensbestimmungen zur Feststellung der Polizeidienstunfähigkeit aufzunehmen.

— Eine Eingabe betraf die Durchführung einer *Prüfung durch den Bundesrechnungshof* im Geschäftsbereich des Bundesministers für Post und Telekommunikation. Im Rahmen einer Analyse von Personalausfällen aus Krankheitsgründen wurde eine Vielzahl personenbezogener Daten der Beschäftigten von den betroffenen Ämtern in Listenform zusammengestellt. Die Listen wurden unter Abtrennung der Spalte „Namen", die in den einzelnen Ämtern verblieb, den Vorprüfungsstellen der Oberpostdirektionen zugeleitet, die die Listen im Auftrag des Bundesrechnungshofes auswerteten. Die Namensspalten werden nach Eingabe der Daten in die Datenverarbeitungsanlage durch die Ämter, die übrigen Erhebungsbögen nach Abschluß des Prüfungsverfahrens vernichtet. Ich habe das Verfahren der Erstellung und Verwendung der Personallisten unter Berücksichtigung des Grundsatzes des Personalaktengeheimnisses sowie des Rechts auf informationelle Selbstbestimmung der betroffenen Beschäftigten als problematisch angesehen. Es begründet die Gefahr, daß auch bei getrennter Aufbewahrung der Namen — insbesondere bei kleineren Dienststellen — eine Reidentifizierung des einzelnen Mitarbeiters anhand der übrigen Personaldaten ohne weiteres möglich ist. Um zu vermeiden, daß Mehrexemplare der Erhebungsbögen für personalwirtschaftliche Maßnahmen ausgewertet, insbesondere zur Leistungs- und Verhaltenskontrolle genutzt werden, habe ich dem BMPT empfohlen, auf die Vernichtung der Mehrexemplare hinzuwirken. Der BMPT hat daraufhin eine entsprechende Verfügung an seine nachgeordneten Stellen erlassen.

— Eine Personalvertretung wandte sich an mich mit der Bitte um datenschutzrechtliche Überprüfung einer im Auftrag des BMPT durchgeführten *Krankenstandserhebung*. Die Ergebnisse der Strukturuntersuchung in einzelnen Ämtern sollten Grundlage für den Entwurf einer „Arbeitsanweisung zur Beobachtung des Krankenstandes" des BMPT sein. Die Erhebung wurde in der Weise durchgeführt, daß in vier Ämtern von der Personalstelle Listen mit Personaldaten erstellt wurden, die u. a. Namen und Zahl der Krankentage in den Jahren 1984 bis 1986 enthielten. Ein Vertreter des BMPT wertete die Listen in den Ämtern aus. Beabsichtigt war, die Listen bis zum Abschluß der Untersuchung im Frühjahr 1989 im jeweiligen Amt aufzubewahren.

Da nach Aussage des BMPT eine Überprüfung von Einzelfällen zu keinem Zeitpunkt der Erhe-

bung vorgesehen war, war die namentliche Bezeichnung aller Mitarbeiter in den Listen nicht erforderlich. Zur Kontrolle der Zuverlässigkeit der Erhebung hätte es ausgereicht, Namen nur in Einzelfällen anzugeben. Die Aufbewahrung der Listen in den einzelnen Ämtern begründet Mißbrauchsmöglichkeiten, z. B. bei Heranziehung im Rahmen von Personalentscheidungen.

Der BMPT hat mir inzwischen zugesichert, daß die Listen nunmehr im Ministerium aufbewahrt werden sollen. Die Namen der Mitarbeiter in den Listen sollen außerdem unkenntlich gemacht werden. Ich habe darum gebeten, mich an der weiteren Vorbereitung der „Arbeitsanweisung zur Beobachtung des Krankenstandes" zu beteiligen.

7 Post und Telekommunikation

Unverändert groß ist die Anzahl der Bürger, die sich telefonisch und schriftlich mit Anliegen an mich wenden, die den Bereich der Deutschen Bundespost betreffen. Oftmals brauche ich den Betroffenen lediglich die sachlichen Gründe und die Rechtsgrundlage einer von ihnen kritisierten Datenverarbeitung zu erläutern. Dabei ist nicht selten festzustellen, daß die Deutsche Bundespost durch bessere Erläuterung und Beratung nicht nur zur Akzeptanz von Maßnahmen, sondern auch zu unter Datenschutzaspekten wünschenswerter Transparenz beitragen könnte.

Die Zusammenarbeit mit dem Bundesministerium für Post und Telekommunikation war gekennzeichnet von Verbesserungen sowohl des Arbeitsklimas als auch des Informationsflusses. Einen wichtigen Beitrag hierzu leisteten regelmäßige Besprechungen über Schwerpunktprobleme zwischen dem für den Datenschutz zuständigen Abteilungsleiter und mir. Dadurch konnten für viele Probleme datenschutzgerechte und praktische Lösungen gefunden werden. In der für die Zukunft besonders wichtigen Frage „Speicherung von Telefonverbindungsdaten" (s. 7.2.3) sind die Standpunkte aber fast unverändert kontrovers.

Begrüßt habe ich, daß Vertreter des Ministeriums an von mir durchgeführten Datenschutzkontrollen gemäß § 19 Abs. 1 BDSG teilnahmen, denn auch dies förderte das gegenseitige Verständnis für die unterschiedlichen Aufgaben.

7.1 Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost

In meinem Elften Tätigkeitsbericht (11. TB S. 30f.) hatte ich dargelegt, daß ich wegen nicht rechtzeitiger Beteiligung zu dem Kabinettsentwurf eines Gesetzes zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost (Poststrukturgesetz) erst nachträglich Stellung nehmen konnte. Im Rahmen einer Anhörung des Ausschusses für das Post- und Fernmeldewesen des Deutschen Bundestages im November 1988 hatte ich Gelegenheit, meine datenschutzrechtlichen Überlegungen vorzutragen. Der Ausschuß bat mich daraufhin, für seine weiteren Beratungen meine Vorstellungen über datenschutzgerechte Vorschriften im Gesetzentwurf zu formulieren. Nach kurzen, aber intensiven Gesprächen — insbesondere mit dem BMP und dem BMJ — konnte ich dem Ausschuß einen entsprechenden Vorschlag vorlegen.

Auch im weiteren Verlauf der parlamentarischen Behandlung des Gesetzentwurfes hatte ich mehrfach Gelegenheit, zu datenschutzrelevanten Aspekten des Entwurfs Stellung zu nehmen und an Formulierungsvorschlägen mitzuwirken. Am 7. April 1989 beschloß der Ausschuß für das Post- und Fernmeldewesen Änderungen des Gesetzentwurfs, die vom Deutschen Bundestag am 20. April 1989 angenommen wurden. Nach Zustimmung durch den Bundesrat am 12. Mai 1989 wurde das Poststrukturgesetz am 8. Juni 1989 im Bundesgesetzblatt verkündet (BGBl I Seite 1026ff.); es trat am 1. Juli 1989 in Kraft.

Das Gesetz geht einerseits von den Arbeitsergebnissen der im Jahre 1985 eingesetzten Regierungskommission Fernmeldewesen, andererseits von den im „Grünbuch" der Kommission der Europäischen Gemeinschaften festgelegten Richtlinien und Prinzipien der Telekommunikation für die europäischen Länder aus. Ziele der darin enthaltenen Empfehlungen waren zum einen die organisatorische Trennung zwischen der Wahrnehmung hoheitlicher Aufgaben und der unternehmerischen Durchführung der Telekommunikationsdienste. Zum anderen sollte der Markt der Telekommunikation der freien Konkurrenz geöffnet werden. Auf die bei solchen Regelungen notwendigen Anpassungen der einschlägigen Datenschutzvorschriften gingen die Empfehlungen nicht ein.

Den Strukturvorschlägen der EG-Kommission folgend sieht das Poststrukturgesetz die Trennung der Hoheitsaufgaben, die vom Bundesministerium für Post und Telekommunikation wahrzunehmen sind, von den Unternehmensaufgaben der Deutschen Bundespost vor, für die drei öffentliche Unternehmen, nämlich die Deutsche Bundespost POSTDIENST, die Deutsche Bundespost POSTBANK und die Deutsche Bundespost TELEKOM geschaffen wurden. Die Öffnung eines Teils des Marktes der Telekommunikationsdienstleistungen für den Wettbewerb bedeutet: Übertragungsnetz und Telefondienst bleiben im Monopol der Deutschen Bundespost, sonstige Telekommunikationsdienste und der Endgerätemarkt werden dem Wettbewerb geöffnet.

Die aus Datenschutzgesichtspunkten entstandenen Besorgnisse bezogen sich hauptsächlich darauf, daß künftig Telekommunikationsdienste im Wettbewerb nicht nur von der DBP TELEKOM, sondern in zunehmendem Maße auch von Privaten angeboten werden. Der Gesetzentwurf der Bundesregierung enthielt zwar Bestimmungen, die es ermöglicht hätten, den bisherigen Datenschutzstandard bei der Deutschen Bundespost zu erhalten, aber keine ausreichenden Bestimmungen über den Datenschutz bei den privaten Telekommunikationsdiensten.

Das Ergebnis meiner Bemühungen im Gesetzgebungsverfahren ist, daß das Gesetz nun die Bundesregierung *verpflichtet*, bereichspezifische Datenschutzvorschriften zu erlassen. Solche Vorschriften haben

dem Grundsatz der Verhältnismäßigkeit, insbesondere der Beschränkung der Erhebung und Verarbeitung personenbezogener Daten auf das Erforderliche sowie dem Grundsatz der Zweckbindung, Rechnung zu tragen. Interessen der jeweiligen Unternehmen dürfen nur soweit berücksichtigt werden, wie diese Grundsätze gewahrt bleiben. Den Datenschutz sichernde Vorschriften müssen nicht nur für die Unternehmen der Deutschen Bundespost, sondern auch für die privaten Anbieter von Telekommunikationsdienstleistungen erlassen werden.

Aus Sicht des Datenschutzes wäre zu wünschen gewesen, daß auch die *Kontrolle* der Einhaltung der datenschutzrechtlichen Vorschriften bei den privaten Telekommunikationsdiensten in gleichwertiger Weise wie bei der DBP TELEKOM vorgesehen worden wäre. Dieser Forderung trägt das Gesetz jedoch nicht Rechnung; es bleibt nicht nur bei den im Bundesdatenschutzgesetz festgelegten Kontrollzuständigkeiten, sondern auch bei den für die Deutsche Bundespost und die Privatunternehmen unterschiedlichen Voraussetzungen und Inhalten datenschutzrechtlicher Kontrollen.

Besondere Bedeutung kommt dem Schutz der Kommunikations*inhalte* zu, da die neuen Techniken deren Speichern zumindest erleichtern. Für alle „Erbringer von Telekommunikationsdienstleistungen" — also sowohl für die DBP TELEKOM als auch für private Unternehmen — bestimmt nun § 14 a Abs. 1 des Fernmeldeanlagengesetzes, daß „Nachrichteninhalte nur aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden (dürfen), soweit dies Gegenstand oder aus verarbeitungstechnischen Gründen Bestandteil der Dienstleistung ist." Damit ist die Speicherung von Nachrichteninhalten aus anderen Gründen — etwa für „betriebliche Zwecke" — unzulässig. Die Bundesregierung wird überdies verpflichtet, für die Speicherung von Nachrichteninhalten — soweit diese erfolgt — bereichspezifische Datenschutzvorschriften zu erlassen, und zwar sowohl für die DBP TELEKOM als auch für private Anbieter. Damit ist einer von mir wiederholt erhobenen datenschutzrechtlichen Forderung Rechnung getragen worden.

Ein weiterer wichtiger Gesichtspunkt war die Sicherstellung der Einhaltung des grundgesetzlich geschützten Fernmeldegeheimnisses. Zu diesem Zweck wurde auf meinen Vorschlag durch eine Änderung des § 10 des Fernmeldeanlagengesetzes klargestellt, daß nicht nur die Bediensteten der DBP TELEKOM, sondern „jeder, der eine für den öffentlichen Verkehr bestimmte Fernmeldeanlage betreibt, beaufsichtigt, bedient und sonst bei ihrem Betrieb tätig ist, zur Wahrung des Fernmeldegeheimnisses verpflichtet" ist.

Mit den hier beschriebenen Änderungen des Regierungsentwurfs des Poststrukturgesetzes ist es gelungen, trotz der ungünstigen Ausgangslage befriedigende Regelungen für den Datenschutz zu erreichen. Entscheidend für diesen Erfolg waren das Interesse an Datenschutzfragen in den Ausschüssen des Deutschen Bundestages, insbesondere im Innenausschuß und im Postausschuß, und die Bereitschaft, trotz des großen Zeitdrucks die notwendigen Regelungen noch aufzunehmen. Für die einzelnen Telekommunikationsdienste stehen die Konkretisierungen durch die zu erlassenden Rechtsverordnungen zwar noch aus. Die gesetzlichen Vorgaben bieten aber eine geeignete Grundlage dafür, daß bei der Weiterentwicklung der Telekommunikation sowohl bei der Deutschen Bundespost als auch bei den privaten Anbietern solcher Dienstleistungen der Datenschutz angemessen berücksichtigt werden kann.

7.2 Digitalisierung der Telekommunikation

7.2.1 Digitalisierung der Nachrichteninhalte

Seit der Erfindung des Telefons vor über hundert Jahren blieb das technische Grundprinzip der Sprachübermittlung unverändert: Tonhöhe und Lautstärke des gesprochenen Wortes veranlassen einen elektrischen Strom zu analogen Schwankungen, die — nach erforderlicher Verstärkung — auf der Empfängerseite wieder in hörbare Sprache umgewandelt werden. Diese sogenannte „analoge" Übertragungstechnik hat grundsätzliche Schwächen, die einer Erhöhung der Übertragungsqualität sowie einer Verbesserung der Leitungsauslastung entgegenstehen. Vor einigen Jahren verließ die Deutsche Bundespost dieses technische Grundprinzip, als sie zunächst bei der Übertragung zwischen ihren Netzknoten auf digitale Verfahren umstellte. Für Teilnehmeranschlüsse wurde diese Neuerung erst im März des Berichtsjahres angeboten, als die DBP offiziell die erste Ausbaustufe des ISDN-Netzes in Betrieb nahm (s. u. Nr. 7.2.3). Eine digitale Steuerung des Verbindungsaufbaus, d. h. des Zusammenschaltens der einzelnen Leitungsstücke zwischen Anrufer und Angerufenem entsprechend der gewählten Nummer, erfolgte zwar bereits seit 1978 in den Telefon-Ortsvermittlungsstellen der DBP, die mit dem Elektronischen Wählsystem (EWS) ausgestattet sind, aber sowohl bei diesem als auch bei der seit etwa 1985 eingesetzten digitalen Vermittlungstechnik (DIVO) wird die Sprache nach wie vor analog übertragen. Anders ist es bei der ISDN-Technik, die nicht nur von der DBP, sondern bereits seit einigen Jahren in zahlreichen privaten Telefonanlagen in Betrieben und Verwaltungen eingesetzt wird. Dabei wird bereits im Telefonapparat das analoge Sprachsignal „digitalisiert": In jeder Sekunde wird die Lautstärke viele tausend mal gemessen und jedem Meßwert eine digitale „Nummer" zugeordnet. Diese Nummern bezeichnen also nicht die Buchstaben, mit denen ein Wort geschrieben wird, sondern die Töne, aus denen das Klangbild zusammengesetzt werden kann. Auf den Leitungen und in den Vermittlungsrechnern der DBP werden dann lediglich diese „Nummern" als kontinuierlicher Datenfluß übertragen. Störungen und Verfälschungen des Datenflusses können dabei unter Anwendung bekannter Verfahren der automatisierten Datenübertragung in weitem Umfang ausgeglichen und korrigiert werden. Auf der Empfangsseite werden den einzelnen „Nummern" dieselben Lautstärkewerte zugeordnet und hieraus — zur Hörbarmachung im Telefonhörer — wieder entsprechende Stromschwankungen erzeugt.

Diese Digitalisierung des gesprochenen Wortes ermöglicht nicht nur eine Erhöhung der Übertragungsqualität und verbesserte Ausnutzung der Übertra-

gungswege, sondern grundsätzlich auch die Verarbeitung solcher Informationen in den elektronischen Datenverarbeitungsanlagen. Dabei ist in erster Linie an die Vermittlungsrechner der DBP zu denken, in denen die Sprache lediglich vom Sprecher zum Hörer „hindurchgeschoben" und dabei nur für tausendstel Sekunden gespeichert wird.

Wenn die technischen Probleme der Spracherkennung und der Inhaltsanalyse von gesprochenen Texten einmal gelöst sind, könnte allerdings diese Speicherung auch z. B. zu einer verstärkten Kontrolle durch hierzu ermächtigte Strafverfolgungs- und Sicherheitsorgane genutzt werden: Während derzeit aufgrund faktisch-technischer Zwänge die Überwachung von Telefonaten wegen des sehr hohen Aufwandes nur in begrenztem Umfang möglich ist, kann dies möglicherweise in naher Zukunft um ein vielfaches ausgeweitet werden. Zu denken ist dabei an automatisch laufende Programme, die den Telefonverkehr zwischen zwei Anschlüssen oder in ausgewählte Länder ständig im Hinblick auf bestimmte Wörter oder Wortkombinationen überwachen und lediglich bei deren Auftreten den vollständigen Inhalt eines Telefonates registrieren.

Programme zur automatischen Wort- und Spracherkennung könnten sich verstärkt auf die Persönlichkeitsrechte von Betroffenen auswirken, wenn die Sprache längerfristig auf Datenträgern gespeichert und ausgewertet wird, z. B. auch durch Unbefugte im Rahmen des „Anzapfens" einer Leitung.

Zum gegenwärtigen Stand der Entwicklung ist festzustellen, daß von den großen EDV-Herstellern und einigen Hochschulen verschiedenartige Spracherkennungsprogramme erprobt werden, deren Leistungsfähigkeit jedoch noch sehr begrenzt ist. Die höchste Erkennungssicherheit leisten dabei Programme, die auf einen ganz bestimmten Sprecher und auf ein eng umrissenes Fachgebiet „trainiert" worden sind, wenn der Sprecher sich darum bemüht, daß seine Sprache erkannt wird. Dazu muß er möglichst so sprechen, wie während des „Trainings", und er muß die einzelnen gesprochenen Wörter so voneinander durch kleine Pausen trennen, daß die Wortgrenzen vom Programm erkannt werden können. Programme, die versuchsweise Sätze verschiedener Sprecher aus einem nicht umrissenen Fachgebiet erkennen sollen, befinden sich demgegenüber noch in einem Versuchsstadium, das eine praktische Anwendung vorerst nicht erwarten läßt. Gleichwohl werden solche Entwicklungen mit großer Aufmerksamkeit zu verfolgen sein, um rechtzeitig — auch gesetzgeberische — Maßnahmen mit dem Ziel eines möglichst sicheren Ausschlusses von Gefahren für die Privatsphäre des Bürgers einzuleiten.

Außer den Verfahren, Sprache zum Zwecke des einfacheren Transports zu digitalisieren, gibt es noch einen anderen Trend zur Digitalisierung von Nachrichten, nämlich die zunehmende Übertragung von Daten, die bereits vor der Übertragung digitalisiert vorliegen und für die deshalb die Umformung in eine digitale Darstellung gar nicht erst erforderlich ist. Es handelt sich um Nachrichten, die von Computern an Computer gesendet werden und die deshalb auch leicht von anderen Computern interpretiert werden können. Solche Nachrichten können größere Lieferungen im industriellen Bereich, aber auch Bestellvorgänge einzelner Personen oder den Austausch von personenbezogenen Daten zwischen öffentlichen oder privaten Verwaltungen, z. B. beim bargeldlosen Zahlungsverkehr, betreffen; auch die briefähnlichen Nachrichten im Btx-Mitteilungsdienst sind in diesem Sinne digitalisiert. All dies zeigt, daß die Zunahme moderner Kommunikationsverfahren auch zum Abbau der technischen Schwierigkeiten einer automatisierten Überwachung führt.

Vor dem Hintergrund dieser Entwicklung und der Öffnung des Telekommunikationsmarktes für private Anbieter habe ich mich bei der Beratung des Poststrukturgesetzes deshalb dafür eingesetzt, daß durch eine Änderung des Fernmeldeanlagengesetzes die rechtlichen Vorkehrungen gegen eine mißbräuchliche Nutzung von Nachrichteninhalten verbessert worden sind (s.o. Nr. 7.1).

7.2.2 Digitalisierung der Verbindungssteuerung

Schon seit langem wird in der sog. analogen Technik der Verbindungsaufbau beim Telefonieren „digital", d. h. mit dem Finger (lat.: digitus) in der Wählscheibe herbeigeführt. Und seit vielen Jahren erfolgt er — im Selbstwählverkehr — auch automatisch: Durch die Wahl einer Ziffer wird z. B. in der weitverbreiteten konventionellen EMD-Vermittlungstechnik ein elektrischer Motor so lange in Betrieb gesetzt, bis er einen Schalter in die Position bewegt hat, die dieser Ziffer entspricht. Damit wird dann schrittweise die gewählte Leitungsverbindung geschaltet.

Mit Digitalisierung der Verbindungssteuerung bezeichnet man jedoch erst die Technik, in der die Verbindung statt durch motorbetriebene Schalter durch einen Computer hergestellt wird. Damit das geschehen kann, muß der Computer die Nummer des anzurufenden Anschlusses zunächst vorübergehend speichern, um dann durch sein Programm die Verbindung herzustellen.

Anders als in der konventionellen Vermittlungstechnik, in der nach dem Ende der Verbindung die Schalter wieder in ihre Ausgangsposition zurückgehen und ohne besondere Zusatzeinrichtungen dann keine Information über die Nummer des Angerufenen mehr vorhanden ist, kann die einmal im Computer gespeicherte Nummer dort festgehalten und leicht noch zu anderen Zwecken verwendet werden, auch wenn die Verbindung inzwischen längst beendet ist. Zugleich können außer der Nummer des Anrufers auch noch der Beginn und das Ende (oder die Dauer) der Verbindung festgehalten werden. Dies ermöglicht es z. B., für den Kunden eine genaue Aufstellung der von ihm zu bezahlenden Verbindungsgebühren anzufertigen oder ihm wenigstens im Reklamationsfall eine solche Aufstellung zum Beweis der Richtigkeit der Gebührensumme vorzuhalten.

Es ist auch möglich, die Verbindungsgebühren nicht mehr wie bisher aus den während einer bestehenden Verbindung erzeugten Gebührenimpulsen nur nach der Zahl der verbrauchten Einheiten in einem Zähler zu sammeln, sondern aus den Verbindungsdaten die

Gebühren zu errechnen. Weil dies auch noch lange nach dem Ende der Verbindung möglich ist, kann man den Vermittlungsrechner von der Gebührenverwaltung entlasten und auch kompliziertere Gebührenstrukturen der Abrechnung zugrunde legen.

Je nach den einzelnen Interessen mögen die weiteren Nutzungen der bei der Digitalisierung der Verbindungssteuerung anfallenden Daten sinnvoll erscheinen. Es darf aber nicht übersehen werden, daß eine vollständige Speicherung nur aller Telefonverbindungsdaten eine Sammlung von vielen Milliarden Datensätzen pro Monat zur Folge hätte, die genau Auskunft darüber gibt, zwischen welchen Anschlüssen wann und wie lange eine Verbindung bestanden hat.

Deshalb beklagen nicht nur technikkritische Bürger, daß mit der — wahrscheinlich unvermeidlichen — Automatisierung in allen Bereichen von Wirtschaft und Verwaltung eine ständig intensivierte und verfeinerte Registrierung vieler Eigenschaften und Handlungen des einzelnen einhergeht; das Schreckgespenst des „Gläsernen Menschen" wird möglich. Von besonderer Bedeutung ist bei solchen Überlegungen zweifellos die zwischenmenschliche Kommunikation, die sich im Zeitalter der elektronischen Datenverarbeitung anscheinend unvermeidbar vom direkten Gespräch und handgeschriebenen Brief hinweg in Richtung auf das Telefonat und andere elektronische Kommunikationsformen bewegt. Dadurch gewinnt der Artikel 10 des Grundgesetzes, der jedem Bürger eine — insbesondere vom Staat — unbeobachtete Kommunikation garantiert, ständig wachsende Bedeutung. Wenn nun im Rahmen der Modernisierung des Telefon- und Datennetzes von der Deutschen Bundespost solche Konzepte ausgewählt werden, die gerade eine lückenlose Registrierung aller technischen Kommunikationsvorgänge bedingen, so muß dies auf grundsätzliche Bedenken stoßen. Das „Grundrecht auf unbeobachtete Kommunikation" verlangt Konzepte, die dies gerade vermeiden: So wie im konventionellen Telefonnetz nach Beendigung des Gespräches — außer einer Weiterschaltung des Gebührenzählers — keine Spuren zurückbleiben, so wären ähnlich einfache und damit datenvermeidende Abrechnungsverfahren auch schon bei der Konzipierung des Bildschirmtextdienstes (vgl. 11. TB S. 33 f.) möglich gewesen. Jedenfalls aber darf die Ausgestaltung der digitalen Telefonvermittlungstechnik nicht zu einer umfassenden Verbindungsdatenspeicherung benutzt werden.

7.2.3 Verbindungsdatenspeicherung bei ISDN

Zusätzlich zu dem allen Bürgern bekannten, „normalen" Telefon, das inzwischen allerdings in vielen zum Teil komfortablen Ausführungen erhältlich ist und in der Postsprache „Analoganschluß" heißt, gibt es jetzt auch den moderneren und komfortableren ISDN-Anschluß, der auch „Universalanschluß" genannt wird. Bei dieser Art von Anschlüssen werden sowohl die Digitalisierung aller Kommunikationsinhalte (s. o. 7.2.1) als auch die Digitalisierung der Verbindungssteuerung (s. o. 7.2.2) so konsequent durchgeführt, daß alle nutzbaren Telekommunikationsdienste über dasselbe Netz (ISDN = Integrated Services Digital Network) geführt werden. Diese zunächst nur für die großen Ballungsräumen von der Post vorgesehenen Anschlüsse sollen ab 1993 flächendeckend zur Verfügung stehen. Die Post strebt an, etwa im Jahr 2020 den weit überwiegenden Anteil des Telekommunikationsverkehrs in dieser Technik abzuwickeln. Deshalb ist die Frage, welche Daten dabei wie lange gespeichert werden, schon heute von allgemeiner und grundsätzlicher Bedeutung.

Im Rahmen einer Kontrolle habe ich mich über die Praxis der Verarbeitung der bei ISDN-Verbindungen entstehenden Daten informiert. Dabei hat sich bestätigt, daß die Post über alle von Universalanschlüssen aus gewählten Verbindungen außer einigen technischen Angaben für mehrere Monate die vollständige Rufnummer des Anrufers und des Angerufenen, den Tag, die genaue Zeit und die Dauer der Verbindung speichert. Als Begründung wird von der DBP angegeben, gerade beim ISDN-Anschluß sei es wegen der Vielzahl möglicher Dienste — neben Telefon, Telefax und Teletex auch weitere — technisch wenig sinnvoll, die Gebührenermittlung im Vermittlungsrechner selbst vorzunehmen; vielmehr sei es notwendig, dies in einem zweiten Verarbeitungsschritt außerhalb der Vermittlungsstelle durchzuführen. Diese Argumentation überzeugt nicht. Denn insbesondere die vollständige Nummer des Angerufenen spielt für die Höhe der Gebühren keine Rolle. Zur Berechnung genügt offensichtlich die Nummer des angewählten Ortsnetzes. Im übrigen stehen auch schon während der Verbindung Gebührendaten zur Verfügung. Sie werden wie bisher an den Anschluß des Anrufers gesendet, um dort eine Gebührenberechnung zu ermöglichen, von der in vielen Telefonanlagen auch Gebrauch gemacht wird. Es ist wenig überzeugend, wenn aus der Entscheidung, auf die Nutzung dieser leicht verfügbaren Gebühreninformation zu verzichten, die Notwendigkeit abgeleitet wird, Verbindungsdaten in einem weit größeren Umfang zu speichern.

Deshalb führt die Post als weitere Begründung an, daß sie nur bei ausnahmsloser und vollständiger Speicherung der Verbindungsdaten in der Lage sei, in einem etwaigen Streit mit dem Zahlungspflichtigen die Richtigkeit der Rechnung zu beweisen. Und weil sie durch die neuen Techniken der Datenverarbeitung dazu nun in der Lage sei, müsse sie diese auch so anwenden. Die Post trifft also mit der Verbindungsdatenspeicherung Vorsorge, um in einem möglicherweise kommenden Streit über die Gebührenhöhe mit Details aus der Kommunikation argumentieren zu können. Mit dieser Frage hat sich der Deutsche Bundestag schon einmal, nämlich bei der Beratung meines Sechsten und Siebenten Tätigkeitsberichts auseinandergesetzt, in denen ich Probleme bei der Verbindungsdatenspeicherung dargestellt habe, nachdem ich schon früher über einen nach kurzer Zeit wieder eingestellten Versuch der Post zur Verbindungsdatenspeicherung in einem Vorläufersystem berichtet hatte (s. 5. TB S. 32 f.). In seiner Entschließung vom 10. Dezember 1986 hat der Deutsche Bundestag ausdrücklich die Zusicherung der Deutschen Bundespost begrüßt, „daß es eine Vorratsspeicherung von Verbindungsdaten nicht geben wird" (s. BT-Drucksache 10/6583).

Die auf der Basis dieser Festlegung gestaltete und diese Fragen regelnde Telekommunikationsordnung (TKO) bietet auch keine Rechtsgrundlage für die bei ISDN praktizierte Speicherung: Zwar gestattet die TKO, *Gebührendaten* bis zu 80 Tagen nach Absendung der Fernmelderechnung aufzubewahren (§ 451 Abs. 3 TKO), in der Definition der Gebührendaten in Absatz 1 der Vorschrift sind jedoch weder Zeitpunkt noch Rufnummer des angerufenen Teilnehmers enthalten. Diese bilden vielmehr gemäß § 450 Abs. 1 TKO *Verbindungsdaten,* die gemäß Absatz 2 dieser Vorschrift umgehend nach Beendigung der einzelnen Telefonverbindung zu löschen sind. Auch die von der DBP gegebene Begründung, nach der eine Fortdauer der Speicherung über das Verbindungsende hinaus zur Klärung von Gebührenstreitigkeiten hilfreich sei, führt zu keiner anderen rechtlichen Bewertung. Denn es sind zwar in § 450 Abs. 2 TKO Ausnahmen genannt, die auch eine längere Speicherung von Verbindungsdaten rechtfertigen. Von den dort genannten Möglichkeiten paßt aber allenfalls die wenig präzise formulierte Ausnahme „aus sonstigen betrieblichen Gründen". Die Tatsache, daß eine Speicherung bei ISDN zu relativ geringen Kosten möglich ist, kann aber kein akzeptabler betrieblicher Grund dafür sein, daß aus einer Ausnahme, die für besondere Fälle vorgesehen ist, für den zukünftigen Massendienst die Regel gemacht wird. Deshalb habe ich diese Speicherungspraxis gemäß § 20 BDSG gegenüber dem Bundesminister für Post und Telekommunikation beanstandet.

Bei der Frage, welche Kommunikationsdaten wie lange gespeichert werden dürfen, handelt es sich keineswegs nur um ein abstraktes Rechtsproblem, das für die Bürger keine Bedeutung hat. So haben sich nicht nur einzelne Bürger mit Briefen und Anrufen an mich gewandt, die ihre Besorgnisse im Zusammenhang mit der Vollspeicherung zum Ausdruck gebracht haben und darin — auch wenn derzeit erst relativ wenige Universalanschlüsse bestehen — doch mittelfristig eine Beeinträchtigung ihrer persönlichen Freiheit sehen. Besonders betroffen haben sich auch beratende Institutionen gezeigt, wie z. B. Telefonseelsorgestellen der christlichen Kirchen und AIDS-Beratungsstellen, die eine Beeinträchtigung, wenn nicht gar Vereitelung ihrer Bemühungen befürchten, wenn die Hilfesuchenden damit rechnen müssen, daß ihre Telefonnummer — als Anrufer oder aber auch als Angerufener — von der DBP gespeichert wird. Ähnliche Bedenken dürften auch bei anderen Beratern wie Rechtsanwälten und Ärzten, aber auch bei Abgeordneten und Journalisten bestehen.

Deshalb ist es besonders zu bedauern, daß der Bundesminister für Post und Telekommunikation meine Beanstandung zurückgewiesen und eine Einstellung der Vollspeicherung abgelehnt hat. Er argumentiert außer mit den oben dargelegten Begründungen damit, jeder Inhaber eines Universalanschlusses habe mit seiner Auftragserteilung an die Post in die Speicherung der Verbindungsdaten eingewilligt; die Speicherung sei deshalb zulässig. Aber selbst wenn eine der gesetzlichen Bestimmung in § 3 BDSG genügende Einwilligung des Anschlußinhabers vorläge, fehlte zur Zulässigkeit der Speicherung noch die ebenfalls notwendige Einwilligung derjenigen, die als Angerufene ja ebenfalls von der Datenspeicherung betroffen sind. Deshalb eröffnet auch der Vorschlag des Bundesministers für Post und Telekommunikation, von einer Speicherung der vollständigen Verbindungsdaten (nur) dann abzusehen, wenn der Inhaber des Universalanschlusses sich dagegen entscheidet und damit zugleich die Post von der „Beweispflicht" freistellt, noch keine angemessene Lösung des Problems.

Als Basis für eine den unterschiedlichen Interessen sehr weitgehend Rechnung tragenden Lösung habe ich vorgeschlagen, daß im Regelfall bei der Verbindungsdatenspeicherung die Nummer des angerufenen Anschlusses nur verkürzt gespeichert wird. Dabei sollten mindestens die beiden letzten Ziffern nicht gespeichert werden. Damit wäre der Angerufene von einem Unbeteiligten kaum noch herauszufinden, aber der Anrufer könnte sich bei gutem Willen in der Regel noch anhand der verfügbaren Ziffern an das Gespräch erinnern, zumindest wenn es teuer (lang) war.

Eine solche Speicherung dürfte auch als Beweis für die erbrachte Verbindungsleistung ausreichen, weil die fehlenden Ziffern für die Zahlungspflicht ohne Bedeutung sind. Und wenn aus Rechtsgründen im Regelfall nicht mehr gespeichert werden darf, kann der Postkunde auch keinen weitergehenden Beweis verlangen. Im übrigen bleibt die Aufschreibung durch den Anrufer oder die Speicherung von Verbindungsdaten in dessen eigener Telefonanlage als Mittel für den Anrufer von der Entscheidung der Post unberührt.

Von der normalerweise vorzunehmenden Speicherung durch die Post könnte in einigen Sonderfällen abgewichen werden:

- Wenn der angerufene Anschluß die Telefonseelsorge (Nummern 11101 und 11102) ist, müßten wegen der Besonderheit — dreimal „1" am Anfang — mindestens die letzten *drei* Ziffern entfallen. Damit wären diese Anrufe nicht mehr von Anrufen von Telefonansagen zu unterscheiden, wenn auch in diesen Fällen nur „11" gespeichert wird.
- Wenn der angerufene Anschlußinhaber die Gesprächsgebühren ganz oder teilweise übernimmt, wird seine vollständige Nummer zur Gebührenzurechnung benötigt.
- Wenn bei bestimmten Datenübertragungsdiensten die Gebühren von der Nummer des angewählten Anschlusses abhängen, müßte diese auch gespeichert werden.
- Entsprechend einem (besonders begründeten) Wunsch eines Anschlußinhabers könnte in Einzelfällen eine weitergehende Speicherung erfolgen.
- Auf Wunsch des Anschlußinhabers könnte die Speicherung reduziert werden.

Auch weitere Sonderfälle, z. B. aus technischen Gründen, könnten berücksichtigt werden, weil die moderne Datenverarbeitung keineswegs verlangt, daß in allen Fällen gleich verfahren wird, sondern im Gegenteil sehr wohl Anpassungen an die jeweiligen Bedingungen und damit weitgehend auch Selbstbestim-

mung erlaubt. Daß solche Lösungen realisierbar sind, weiß ich aus Diskussionen mit Fachleuten der Nachrichtentechnik und der zugehörigen Datenverarbeitung.

Der Bundesminister für Post und Telekommunikation hat sich zu einer solchen Lösung (bisher) leider nicht entschließen können; er fördert damit ohne Not Widerstände gegen die Durchsetzung der ISDN-Technik, weil diese Technik bei dem derzeit verfolgten Konzept der Speicherung von Verbindungsdaten mit dem Ende des unregistrierten Telefonierens verbunden wird.

7.3 Mobile Funkanlagen

Wie oben dargelegt haben sich beim „normalen", drahtgebundenen Telefon erst in den letzten Jahren durch technische Weiterentwicklungen ernstere datenschutzrechtliche Probleme ergeben: Da früher keine automatisierten Registrierungen vorgenommen wurden, entstanden zunächst auch keine zu schützenden personenbezogenen Daten. Ganz anders sah dies von Anfang an beim Funktelefon („Autotelefon") und anderen mobilen Funkdiensten aus, bei denen zumindest vorübergehend stets alle die Verbindung beschreibenden Daten — einschließlich der Rufnummern der Beteiligten — registriert werden mußten. Die sich daraus ergebenden Datenschutzprobleme wurden in der Vergangenheit von mancher Seite schon wegen „quantitativer Geringfügigkeit" nicht sehr ernst genommen. In der Tat war die technische Kapazität des — lange Jahre einzigen — Funktelefonnetzes B auf 26 000 Teilnehmer begrenzt; die hohen Kosten machten ein Autotelefon überdies für den Normalbürger nahezu unerschwinglich. Für das 1985 in Betrieb gegangene Nachfolge-Funktelefonnetz C wird aber bereits für 1992 der Maximalausbau von nahezu 500 000 Teilnehmern erwartet. Für das nachfolgende paneuropäische digitale D-Netz werden im Jahr 2000 in der Bundesrepublik Deutschland 1,5 bis 2 Millionen Teilnehmer und europaweit 16 Millionen Geräte geschätzt. Beim Cityruf rechnet die Deutsche Bundespost bereits 1993 mit 430 000 Teilnehmern. Diese Entwicklung wird nicht nur ermöglicht und unterstützt durch die mit wachsenden Stückzahlen drastisch sinkenden Preise, sondern auch durch den gerade in diesem Bereich erwarteten Wettbewerbsdruck seitens privater Anbieter (siehe oben Nr. 7.1). Angesichts dieser Entwicklungen kann auch der Datenschutz bei mobilen Funkdiensten nicht mehr als ein eher exotisches Problem einer kleinen Gruppe angesehen werden.

7.3.1 Funktelefondienst

Insbesondere wegen der praktizierten Vollspeicherung der Telefonverbindungsdaten sowie der langen Speicherungsdauer habe ich den Funktelefondienst der DBP in den vergangenen Jahren wiederholt kritisieren müssen. In meinem Elften Tätigkeitsbericht (s. 11. TB S. 30ff.) habe ich über meine datenschutzrechtliche Kontrolle des C-Netzes sowie die förmlichen Beanstandungen berichtet, die ich gegenüber dem Bundesminister für Post und Telekommunikation vorzubringen hatte. Schwerpunkte dabei waren zum einen von der Telekommunikationsordnung nicht gedeckte Speicherungen (u. a. der Telefonnummer des Angerufenen), zum anderen das Fortdauern der Speicherung der Daten aller Verbindungen bis zu einer Gesamtzeit von etwa drei Monaten und die Einrichtung von Verfahren zur Übermittlung der gespeicherten Daten an Stellen, für die die Kenntnis dieser Daten nicht erforderlich ist.

Der BMPT hat für die Übermittlung der gespeicherten Daten restriktive Regelungen eingeführt aber im übrigen meine Beanstandungen zurückgewiesen und ausgeführt, daß sowohl die detaillierte, umfassende Registrierung der Verbindungsdaten als auch deren lange Speicherungsdauer unerläßlich seien. Er verwendet in diesem Zusammenhang die gleichen Argumente wie bei dem 1972 in Betrieb gegangenen B-Netz. Grundaussage ist dabei, die technischen Eigenschaften eines Funktelefonnetzes erhöhten erheblich die Möglichkeiten mißbräuchlicher Benutzung und anderer manipulativer Eingriffe gegenüber dem drahtgebundenen Netz. Daher müßten unter anderem stets die Verbindungsdaten aller Verbindungen registriert und unter dem Gesichtspunkt von Inplausibilitäten und möglichen oder wahrscheinlichen Mißbräuchen, aber auch im Hinblick auf etwaige von der DBP zu vertretende gebührenrelevante Fehler analysiert werden.

Bereits beim B-Netz hatte ich mich kritisch zur Vollspeicherung der Verbindungsdaten geäußert (7. TB S. 25f.) und gefordert, bei dem damals geplanten neuen System die Mißbrauchsmöglichkeiten so zu vermindern, daß diese Speicherung nicht mehr notwendig ist. Im April dieses Jahres habe ich die Auswertung der Verbindungsdaten des alten B-Netzes zum Zwecke der Mißbrauchserkennung und -aufklärung datenschutzrechtlich kontrolliert. Ich habe dabei den Eindruck gewonnen, daß die eingesetzten EDV-Programme nur die Verbindungsdaten derjenigen Funktelefonate weiterverarbeiten, für die tatsächliche Anhaltspunkte für mißbräuchliche Benutzung — etwa durch Verwendung manipulierter Funktelefongeräte — oder aber für technische Störungen vorliegen. Die von der betreffenden Dienststelle der DBP vorgelegten Erfolgszahlen belegten dabei die Wirksamkeit und damit auch die Erforderlichkeit dieses Verfahrens.

Anders ist die gegenwärtige Praxis bei dem erst 1985 in Betrieb gegangenen C-Netz zu bewerten: Hier ist — wie bereits in meinem Elften Tätigkeitsbericht dargestellt (s. o.) — die Benutzung eines Funktelefongerätes nur mit einer (Speicherchip-)Berechtigungskarte möglich, die in einem gesicherten Verfahren dem Berechtigten zugesandt wird. Das unberechtigte Registrieren des Funkverkehrs — etwa zur Ausspähung der Sicherungsnummer — ist durch ein Verschleierungsverfahren wesentlich erschwert. Anders als im B-Netz kann überdies bei Mißbrauchsverdacht die betreffende Funktelefonnummer sofort gesperrt werden. Schon von daher können die dargelegten bisherigen Argumente eine Vollspeicherung im C-Netz nicht mehr rechtfertigen.

Tatsächlich konnte ich feststellen, daß die Verbindungsdaten des C-Netzes — anders als im B-Netz — bislang nicht systematisch automatisiert ausgewertet werden, sondern daß dies vielmehr lediglich im Einzelfall ausnahmsweise und manuell erfolgt. Mir wurde allerdings mitgeteilt, daß seit längerer Zeit ein Programmsystem zur Mißbrauchserkennung und -aufklärung entwickelt wird, das demnächst in Betrieb genommen werden soll. Ich hatte den BMPT gebeten, mir anhand konkreter Fallkonstellationen und -zahlen darzulegen, in welcher Weise ein solches Programmsystem angemessen und erforderlich ist, um Mißbrauchsfälle im C-Netz zu erkennen und aufzuklären. Ich habe dabei den Eindruck gewonnen, daß sich die Mißbrauchsproblematik zwar gegenüber dem B-Netz wesentlich verringert hat, gleichwohl aber fortbesteht. Ich halte es auch für möglich, daß mit dem System in bestimmten Fällen nicht nur Mißbräuche erkannt, sondern auch aufgeklärt werden können. Diese Tatsache sowie die Präventivfunktion einer Mißbrauchskontrolle kann daher unter Datenschutzgesichtspunkten — anders als in drahtgebundenen Telekommunikationsnetzen (s. o. Nr. 7.2.2) — die vorübergehende Speicherung auch der Zielnummer rechtfertigen. Jedoch müssen die automatisierten Analyseprogramme so gestaltet sein, daß nur die Verbindungsdaten solcher Gespräche weiterverarbeitet werden, für die nach den Erfahrungen mit erhöhter Wahrscheinlichkeit Mißbrauch in Betracht zu ziehen ist, und die Daten aller übrigen Gespräche — bis auf die zur Rechnungsstellung erforderlichen — unverzüglich gelöscht werden. Der BMPT hat sich jedoch zu einer so differenzierten Behandlung der Verbindungsdaten nicht entschließen können; er beabsichtigt, eine Mißbrauchsanalyse zur Erfassung kritischer Verbindungsdaten durchzuführen und weiterhin die Verbindungsdaten im bisherigen Umfang zu speichern.

Wie bereits erwähnt, soll im Jahre 1991 das paneuropäische digitale Funktelefonnetz nach der GSM-Norm (groupe spéciale mobile) der europäischen Fernmeldeverwaltungen in Betrieb gehen, das in der Bundesrepublik D-Netz heißt. Hier wird übrigens neben dem von der DBP-TELEKOM betriebenen D1-Netz ein weiteres von einem privaten Konsortium unter der Bezeichnung „D2-Netz" errichtet werden. Über die Einführung des paneuropäischen Mobilfunknetzes wurde 1987 ein „Memorandum of Understanding" beschlossen, das bisher 18 europäische Staaten unterzeichnet haben. Wesentliche Merkmale dieses Netzes sind die geplante große Teilnehmerkapazität — über zwei Millionen in der Bundesrepublik Deutschland —, digitale Sprachübertragung, ISDN-Fähigkeit (vgl. oben Nr. 7.2.3) sowie durch europaweite Normung z. B. für einen Bundesbürger die Möglichkeit, mit seinem Autotelefon im Urlaub von Sizilien aus mit einer befreundeten Familie zu telefonieren, die ihrerseits in Norwegen mit dem PKW unterwegs ist. Die dabei gespeicherten Telefonverbindungsdaten werden zunächst von der regionalen Betreibergesellschaft — im Beispiel in Italien — erfaßt und dann der heimatlichen Betreibergesellschaft des Teilnehmers übermittelt. Bei diesem Verfahren wird eine Vielzahl datenschutzrechtlicher Fragen erkennbar, so z. B. nach Art und Umfang der registrierten Daten, Dauer und Sicherung ihrer Aufbewahrung, Art und Sicherheit des Übermittlungsweges und nach dem Schutz gegenüber unbefugtem Zugriff.

Angesichts der im B- und C-Netz seit Jahren bekannten, sich im D-Netz verschärfenden Datenschutzprobleme hätte ich es begrüßt, wenn ich von der DBP so rechtzeitig über datenschutzrelevante Planungen informiert worden wäre, daß ich eine Möglichkeit gehabt hätte, etwaige Einwände in die Planungen einzubringen, solange die technischen Bedingungen noch nicht international festgelegt sind. Bis heute ist dies allerdings nicht geschehen. Ich gehe gleichwohl davon aus, daß die genannten Datenschutzprobleme als solche erkannt und Lösungen hierfür oder zumindest entsprechende Ausgestaltungsrahmen vorgesehen sind.

7.3.2 Cityruf

Die wohl auch noch in Zukunft recht hohen Kosten halten manchen Interessenten von der Anschaffung eines Funktelefongerätes ab. Für viele Zwecke reicht es auch aus, einer dringend zu erreichenden Person eine kurze Botschaft durchgeben zu können, im einfachsten Falle ein Signal, das sie verabredungsgemäß veranlaßt, über das „normale" Telefon eine bestimmte Nummer anzurufen. Seit dem Frühjahr dieses Jahres stellt die Deutsche Bundespost hierfür den Cityrufdienst zur Verfügung, der die jederzeitige Erreichbarkeit eines Teilnehmers — vorerst nur in den Ballungsräumen — sicherstellen soll. 1990 sollen alle Städte über 30 000 Einwohner versorgt sein, und für 1993 werden bereits über 400 000 Teilnehmer erwartet.

Zur ständigen drahtlosen Erreichbarkeit führt der Teilnehmer einen kleinen Funkempfänger mit sich, der kleiner als eine Zigarettenschachtel und nur unwesentlich schwerer ist. Je nach „Komfortklasse" seines Empfängers kann er dann innerhalb des Funkversorgungsgebietes — etwa ganz Berlin (West) — zumindest ein Piepsignal empfangen, dessen Bedeutung natürlich vorher vereinbart sein sollte. Typische Anwendungen betreffen z. B. den Kundendiensttechniker, den die Einsatzzentrale stets und überall auf diese Weise erreichen kann. Dazu muß sie zunächst die Telefonnummer des Cityruf-Dienstes anrufen — z. B. 0164 — und dann die Funknummer des Technikers wählen, um sein Gerät zum Piepen zu bringen und ihn damit zum Telefonanruf in der Zentrale aufzufordern. Im komfortabelsten Falle wird dem Teilnehmer auf einem im Gerät eingebauten Display eine Nachricht angezeigt, die aus bis zu 80 Buchstaben und Zahlen bestehen kann. Um eine solche Nachricht systemgerecht aufzugeben, muß der Absender über einen Personalcomputer mit Postanschluß oder aber ein Bildschirmtextgerät verfügen.

In allen Fällen ist zur Durchführung des Dienstes die Speicherung personenbezogener Daten erforderlich: Im einfachsten Fall lediglich die Tatsache, daß eine Nachricht an das Gerät des Besitzers durchzugeben ist, im letztbeschriebenen Fall zusätzlich die Nachricht selbst. Diese Speicherungen standen im Mittelpunkt erster Erläuterungen des Cityrufdienstes, um

die ich die DBP gebeten hatte. Unter Gesichtspunkten des Datenschutzes stellen sich zum einen Fragen nach der Speicherungsdauer der Nachricht sowie der Verbindungsdaten, zum anderen nach der Sicherheit gegenüber unbefugtem Zugriff auf die Nachricht, etwa durch Abhören des Funkverkehrs.

Ich habe begrüßt, daß die Speicherung der Nachricht systemseitig nur solange erfolgt, bis „der Ruf abgesetzt ist", d. h. vom Sender der DBP das Rufsignal sowie ggf. die Nachricht ausgestrahlt worden sind. Die Löschung erfolgt unmittelbar danach.

Schon aufgrund der kurzen Speicherdauer ist das Risiko eines unbefugten Zugriffes auf die Nachricht im Bereich der Deutschen Bundespost sehr gering. Die Übertragung der Nachrichten auf dem Funkwege erfolgt jedoch unverschlüsselt; die dabei verwendete Codierung ist europaweit standardisiert und bekannt. Daher ist es jedem, der über entsprechende Geräte und Kenntnisse verfügt, ohne großen Aufwand möglich, alle im Cityruf übertragenen Nachrichten abzuhören und auch die Funkgerätenummer des Adressaten festzustellen; dessen Namen wird er in der Regel allerdings zumindest so lange nur schwer ermitteln können, wie die DBP keine Teilnehmerverzeichnisse herausgibt. Aus diesen Gründen ist auch der Mißbrauchsanreiz gering, der darin besteht, ein eigenes Gerät derart zu manipulieren, daß es die für einen Dritten bestimmten Nachrichten anzeigt.

Leider erfolgt die Funkübertragung nicht nur beim Cityruf, sondern allgemein in der Telekommunikation nahezu ausschließlich unverschlüsselt. Angesichts des beschränkten Nachrichtenumfanges einerseits und der zu erwartenden typischen Anwendungen andererseits kann dies beim Cityrufdienst solange hingenommen werden, wie den Betroffenen die Risiken des Abhörens bekannt und die daraus entstehenden Gefahren gering sind. Die heute zur Verfügung stehende Technik ermöglicht jedoch ohne größere Schwierigkeiten eine verschlüsselte Nachrichtenübertragung auf dem Funkwege. Um so unverständlicher ist es, daß weder die DBP noch private Anbieter dem im nennenswerten Maße Rechnung tragen. So ist auch im geplanten Funktelefon-D-Netz (siehe oben Nr. 7.3.1) meines Wissens die kryptographische Verschlüsselung der Sprachübertragung nicht serienmäßig vorgesehen.

7.4 Sprachboxdienst

Besonders für den „beruflichen Telefonierer" ist es häufig wichtig, einem gewünschten Partner unabhängig von dessen Aufenthaltsort und der Tageszeit eine Nachricht zukommen zu lassen und sicher zu sein, daß er sie dann auch wirklich erhält. Der seit Jahren bekannte Telefon-Anrufbeantworter erfüllt diese Forderung nur unzureichend. Seit dem 1. Dezember 1985 hat die Deutsche Bundespost den Versuchsbetrieb des Sprachboxdienstes aufgenommen, der diese Aufgabe besser und sicherer lösen soll. Er ermöglicht es, von jedem Telefon aus dem Inhaber einer elektronischen „Sprachbox" eine gesprochene Nachricht zukommen zu lassen. Der Inhaber der Sprachbox kann diese und weitere in der Zwischenzeit eingegangene Nachrichten von einem Telefon aus jederzeit abhören. Sowohl die Nachrichten selbst als auch die Verbindungsdaten unterliegen dem grundrechtlichen Schutz des Fernmeldegeheimnisses. Im Rahmen einer Datenschutzkontrolle habe ich die Einhaltung der allgemeinen sowie der speziell hierzu erlassenen datenschutzrechtlichen Vorschriften beim Versuchsbetrieb zum Sprachboxdienst in Hannover überprüft.

Beim Sprachboxdienst werden gesprochene Nachrichten digitalisiert (s. o. 7.2.1) und in einem Rechner beim Fernmeldeamt Hannover in einer sog. Sprachbox gespeichert. Sie können vom Inhaber der Sprachbox jederzeit abgerufen und gelöscht werden. Dabei kann die Nachricht grundsätzlich von einem beliebigen Telefon aus — auch im Ausland — in diese Box „hineingesprochen" und vom Boxinhaber ebenso von einem beliebigen Telefon aus abgerufen und gelöscht werden. Voraussetzung ist jedoch, daß es sich bei den verwendeten Telefonen um solche für das Mehrfrequenz-Wählverfahren (MFV) handelt, die zwar im Ausland bereits weit verbreitet, in Deutschland allerdings nur als Sondertelefone erhältlich sind. Zum Abhören der in seiner Sprachbox für ihn hinterlegten Nachrichten muß ein Boxinhaber zunächst die bundeseinheitliche Telefonnummer des Sprachboxdienstes Hannover anrufen und sich dann durch Wahl seiner persönlichen „Identifikationsnummer" — die nur ihm bekannt sein sollte — als berechtigter Benutzer ausweisen. Diese Identifikationsnummer stellt daher gewissermaßen den Schlüssel zum Briefkasten „Sprachbox" dar, der wie jeder Schlüssel nicht nur nachgemacht, sondern auch anderen, insbesondere Unbefugten, zugänglich werden kann. Ein zusätzliches Authentifikationshilfsmittel in Gestalt eines Paßwortes ist daher zur Datensicherung unerläßlich. Zwar ist auch beim Sprachboxdienst die Verwendung eines solchen Paßwortes möglich, die Einrichtung wird jedoch in das Belieben des Betroffenen gestellt, und er wird auch hierzu nicht weiter angehalten. Da nicht jeder Benutzer um die begrenzte Sicherheit der elektronischen Datenfernverarbeitung weiß, habe ich der DBP empfohlen, das System so zu gestalten, daß zunächst die Einrichtung und Verwendung eines Benutzerpaßwortes zwingend verlangt werden. Erst wenn der Benutzer nach Unterrichtung über die vorhandenen Risiken ein solches nicht für erforderlich hält, sollte er die Verwendung von sich aus „ausschalten" können.

Ein Sprachboxteilnehmer kann für einen anderen in dessen Sprachbox eine Nachricht hinterlegen, indem er zunächst die Rufnummer des Sprachboxdienstes wählt und sich durch Eingabe seiner eigenen Identifikationsnummer ausweist. Durch Wahl einer weiteren Kennziffer — für „Eingabe" — und der Sprachboxnummer des gewünschten Adressaten erhält er dann die Möglichkeit, diesem eine Nachricht „hineinzusprechen". Auch einem Nicht-Sprachboxteilnehmer ist dies möglich, indem er sich von einer Bedienkraft („Operator") manuell mit der Sprachbox verbinden läßt, für die die Nachricht bestimmt ist. Dieser Operator gibt auch — wenn gewünscht — den Teilnehmern Hilfen bei der Benutzung.

Den Schwerpunkt der Datenschutzkontrolle bildeten die Möglichkeiten und Berechtigungen sowohl des

Operators als auch des mit der Wartung des Systems befaßten Personals der DBP. Aus den Forderungen der Anlage zu § 6 BDSG ergibt sich, daß für die bei der Datenverarbeitung Tätigen Zugriffs- und Einsichtsrechte nur soweit zulässig sind, wie dies für die jeweilige Aufgabenerledigung unerläßlich ist. Dies wird im allgemeinen durch die Vergabe individueller und aufgabenspezifischer Paßworte erreicht, die von den Beschäftigten selbst gewählt und verändert werden können. Auch der Rechner des Sprachboxdienstes sieht solche Paßworte mit verschiedenen Berechtigungsebenen („Levels") vor. Beim Sprachboxdienst Hannover wurden diese Möglichkeiten jedoch nicht genutzt, vielmehr waren die betreffenden Paßworte allen Bediensteten der Arbeitseinheit bekannt und waren auch seit längerer Zeit unverändert. Damit kann eine wichtige Forderung der Datensicherheit, nämlich daß auch nachträglich stets festgestellt werden kann, wer welche Datenspeicherung wann vorgenommen hat, nicht erfüllt werden. Dies wird insbesondere deshalb problematisch, weil im System auch eine Funktion vorhanden ist, die das Aufheben des gesamten Paßwortschutzes ermöglicht. Weder die Inhalte der Boxen der Teilnehmer noch die Verwaltungsdaten und die Programme wären dann paßwortgeschützt, sie könnten also leicht zur Kenntnis genommen oder willkürlich verändert werden. Nach Wiedereinschalten des Paßwortschutzes würde dieser Mißbrauch zunächst nicht bemerkt, jedenfalls wäre der Urheber nicht nachweisbar. Diese Risiken können möglicherweise während des laufenden Probebetriebes durch Stichprobenkontrollen begrenzt werden; für einen nachfolgenden Wirkbetrieb habe ich jedoch dringend Änderungen empfohlen, u. a. auch automatische Aufschreibungen (logging) zumindest über die Nutzung bestimmter wichtiger Funktionen.

Die Stellungnahme der DBP zu diesen und weiteren Empfehlungen und Anregungen lag mir bei Redaktionsschluß noch nicht vor; mein Kontrollbericht war nur wenige Wochen zuvor an die DBP gesandt worden.

7.5 TEMEX

Seit einigen Jahren nutzt die Deutsche Bundespost die Möglichkeit, auf den für den Telefondienst verlegten Kabeln zu ihren Vermittlungsstellen zusätzliche Signale zu übertragen. Das kann unabhängig davon geschehen, ob gerade jemand das Telefon benutzt, und auch ohne daß dadurch der Telefondienst beeinträchtigt wird. Diese mögliche „Zweitnutzung" bietet nur eine geringe Kapazität; sie reicht aber aus, um damit digital dargestellte Zeichen schnell und von allen Stellen zu übertragen, wohin Telefonkabel verlegt sind, also beinahe von jedem Haus aus. In den Vermittlungsstellen der Post werden diese Signale „herausgefiltert" und je nach ihrer verabredeten Bedeutung weiterverarbeitet.

Eine besonders einfache Anwendung dieses TEMEX (abgeleitet von telemetry exchange) genannten Dienstes ist das Übertragen von Alarmmeldungen, z. B. aus durch Glasbruch- oder Bewegungsmeldern überwachten Räumen, die an Überwachungsdienste weitergeleitet werden, oder auch von Notrufen hilfsbedürftiger Personen, durch die ein entsprechender Hilfsdienst alarmiert wird. Solche Dienstleistungen werden — regional unterschiedlich — schon angeboten, und es zeigt sich, daß die wegen der Nutzung des ohnehin vorhandenen Telefonnetzes relativ geringen Gebühren das Entstehen solcher Angebote fördern.

Mit derselben Technik lassen sich aber nicht nur so einfache Informationen (wie „Zustand normal" oder „Eingreifen erforderlich"), sondern auch Meßwerte z. B. für die Temperatur in einem Lagerraum übertragen. Ebenso wäre es auch möglich, den häuslichen Verbrauch von Wasser und Energie mit für TEMEX geeigneten Zählern zu messen und die Ergebnisse zu Abrechnungszwecken an die jeweiligen Versorgungsunternehmen weiterzuleiten. Und wenn diese Installationen erst einmal geschaffen sind, dann wäre es auch möglich, mit vernachlässigbaren Zusatzkosten den jeweiligen Verbrauch täglich, viertelstündlich oder noch häufiger abzurufen. So verbrauchsnahe Messungen können hilfreich sein, um die Entstehung von Verbrauchsspitzen zu erforschen und Mittel zu ihrer Kappung einzusetzen, z. B. durch Tarife, bei denen der Verbrauch zu den Tageszeiten besonders viel kostet, in denen Spitzenlasten auftreten. Anhand der detaillierten Verbrauchswerte der einzelnen Haushalte wäre es den Versorgungsunternehmen zudem möglich, jeden Verbraucher — orientiert an seinen Verbrauchsgewohnheiten — über seine Möglichkeiten zur Energieeinsparung oder zur Minderung seines Wasserverbrauchs zu beraten.

So interessant solche Anwendungsmöglichkeiten der modernen Technik auch sein mögen, so darf doch nicht übersehen werden, daß hier ein erhebliches Risiko einer Ausforschung des Privatlebens besteht. Und wenn man auch daraus, wann z. B. jemand duscht oder badet, kalt oder warm, morgens sein Brot röstet, mit oder ohne Ei frühstückt, kein Geheimnis machen muß, so stellt sich doch die Frage, ob die Versorgungsunternehmen in der Lage sein sollen, sich das per TEMEX berichten zu lassen, oder ob nicht die Grenzen der allgemein zumutbaren Detaillierung wesentlich früher erreicht sind.

Man kann sicher darüber streiten, wie weit die Deutsche Bundespost als Anbieter des Übertragungsdienstes TEMEX eine Mitverantwortung für dessen datenschutzgerechte Anwendung trägt, ein innerer Zusammenhang zwischen der Bereitstellung dieses Instruments und seiner Nutzung ist jedoch nicht von der Hand zu weisen. Deshalb erhob der Bundesminister der Justiz auch Bedenken gegen eine Änderung der Telekommunikationsordnung, in der — ohne auf einzelne Nutzungen einzugehen — eine Intensivierung der Datenübertragungen im TEMEX-Dienst geregelt werden sollte.

Daraufhin wurden die Probleme und die Lösungsmöglichkeiten gemeinsam von den vorrangig daran interessierten Ressorts (BMJ, BMP, BMI, BMWi) mit Vertretern der Versorgungsunternehmen und mir besprochen. Dabei zeigte sich, daß hier ein ernstzunehmender Regelungsbedarf besteht, um den sinnvollen und akzeptablen Einsatz von TEMEX für die Abrechnung von Versorgungsleistungen zu ermöglichen,

ohne daß damit zugleich unverhältnismäßig viele Daten aus dem häuslichen Bereich Außenstehenden übermittelt und von diesen genutzt werden.

Bei den erwähnten Gesprächen wurden die aufgezeigten Fragen weniger als ein Problem der Datenübertragung durch die Post, sondern eher als ein Problem der Vertragsgestaltung durch die Versorgungsunternehmen angesehen. Dementsprechend sagte der Bundesminister für Wirtschaft zu, etwa Mitte 1990 einen Entwurf für eine Datenschutzvorschrift in den Allgemeinen Versorgungsbedingungen für die Elektrizitäts- und Gasversorgung von Tarifkunden und ggf. auch in den entsprechenden Verordnungen über die Versorgung mit Fernwärme und Wasser vorzulegen. Geplant ist eine Regelung, die normalerweise höchstens eine monatliche Erhebung des jeweiligen Gesamtverbrauches vorsieht, der nach Zeitzonen aufgegliedert sein kann, etwa entsprechend den schon heute gelegentlich vorgenommenen Differenzierungen. Zusätzliche Erhebungen können bei Änderungen der Tarife und des Vertragsverhältnisses erfolgen. Daneben kann mit dem Kunden eine detailliertere Erfassung vereinbart werden, wenn er dies — etwa zur Beratung über den für ihn günstigsten Tarif oder ein zweckmäßiges Verbrauchsverhalten — wünscht.

Ich hoffe, daß eine den verschiedenen Interessen gerecht werdende Lösung bald vorliegt, damit die Versorgungswirtschaft und die Zählerhersteller zuverlässige Planungsgrundlagen erhalten. Im übrigen würde ich es begrüßen, wenn bei neuen Zählern auch Aufzeichnungen oder zumindest Anzeigen des Verbrauches (nur) für die Kunden sichtbar, z. B. direkt am Zähler, eingerichtet werden könnten, weil damit die Kunden selbst und schon während des Verbrauchs die Wirkungen ihres Verhaltens erkennen können.

7.6 Anschriftenprüfung

Über die datenschutzrechtliche Problematik bei der Feststellung der aktuellen Anschrift eines Adressaten und deren Übermittlung an den Absender (Anschriftenprüfung) durch die Deutsche Bundespost habe ich berichtet (5. TB S. 34 und 11. TB S. 36). Aufgrund meiner Bemühungen ist nun das Verfahren der Anschriftenprüfung für den Postkunden transparenter geworden. So enthält § 38 Postordnung seit dem 1. September 1989 einen Hinweis darauf, daß eine geänderte Anschrift Dritten auf Anfrage mitgeteilt werden darf. Die Post wird verpflichtet, den Betroffenen einer Anschriftenprüfung in geeigneter Weise auf sein Recht hinzuweisen, schriftlich der Anschriftenweitergabe zu widersprechen. Diese Neuregelungen halte ich für eine datenschutzrechtlich akzeptable Lösung.

7.7 Ermittlungen durch Postzusteller

Durch eine Eingabe ist mir die bisherige Praxis der Beitreibungsstellen der Fernmeldeämter bekannt geworden, die Postämter per Formschreiben aufzufordern, ihre Postzusteller über persönliche Lebensverhältnisse von Postempfängern zu befragen. Die Zusteller sollten Angaben über Mietverhältnis, Arbeitsstelle, Verschuldung, Krankheit, Alter, Kinderzahl, Kfz und Rente der in ihrem Zustellbezirk wohnenden Postempfänger machen.

Gegenüber dem Bundesminister für Post und Telekommunikation habe ich diese Art der Informationsbeschaffung kritisiert, weil sie zu einer Durchbrechung des Postgeheimnisses und des Amtsgeheimnisses führen kann. Wie ich bereits in früheren Tätigkeitsberichten (8. TB S. 23 und 9. TB S. 34 f.) dargelegt habe, umfaßt die Verschwiegenheitspflicht des Zustellers auch solche Erkenntnisse, die er unmittelbar oder durch Rückschlüsse aus seiner amtlichen Tätigkeit gewinnt. Im vorliegenden Fall hätte der Postzusteller zwangsläufig bei Erledigung des Auftrages einer Beitreibungsstelle auch solche Informationen verwerten müssen, die er den Postsendungen entnommen hat.

Meinen Bedenken hat der Bundesminister für Post und Telekommunikation inzwischen Rechnung getragen. Die bisherige Formblattanfrage der Beitreibungsstelle beim Postamt wurde eingestellt und das Verfahren auf die Prüfung von Anschriftsdaten beschränkt.

7.8 Kontrolle eines Postgiroamtes

Im Berichtsjahr habe ich eine Kontrolle bei einem Postgiroamt durchgeführt. Dabei traten Mängel in der organisatorischen Sicherstellung des Datenschutzes zutage. So konnte die Übersicht gemäß § 15 BDSG über die beim Postgiroamt vorhandenen Dateien vom internen Datenschutzbeauftragten während der viertägigen Kontrolle nicht vorgelegt werden, obwohl — wie sich nachträglich herausgestellt hat — eine solche Übersicht im Amt existierte. Diesen Mangel habe ich gegenüber dem Bundesminister für Post und Telekommunikation beanstandet, weil die zur Sicherstellung des internen Datenschutzes beauftragten Mitarbeiter Kenntnis vom Bestehen der Dateiübersicht haben müssen. Dies ist nicht nur zur Erfüllung der eigenen Aufgaben des Datenschutzbeauftragten unerläßlich, sondern auch zur Erledigung der Pflicht nach § 19 Abs. 3 BDSG, mich zu unterstützen.

Schwerpunkt der Kontrolle bildete die erstmalige Prüfung des Verfahrens der Beantragung, Herstellung und Aushändigung von eurocheque-Karten sowie der Datenverarbeitungsvorgänge beim Abheben von Bargeld am Automaten. Ich konnte dabei feststellen, daß diese Verfahren zwar ausreichend sicher, jedoch in einigen Punkten verbesserungsbedürftig sind.

So wird dem Postgirokunden, der eine eurocheque-Karte beantragt, nicht transparent gemacht, daß seine Girodaten auch in den nicht-öffentlichen Bereich übermittelt werden — z. B. an den Sparkassenverlag, der die Karte herstellt, und an andere eurocheque-Kreditinstitute, mit denen der Postgirodienst eine gemeinsame Evidenzzentrale betreibt. Diese Evidenzzentrale sammelt die Kontosperren sämtlicher am eurocheque-Verfahren beteiligten Kreditinstitute, führt sie zusammen und schafft damit eine allen Instituten zur Verfügung stehende Sperrdatei. Der Bundesminister für Post und Telekommunikation hat inzwischen

zugesichert, künftig die Postkunden mittels neuer Antragsformulare auf die Datenübermittlung zu Zwekken der Herstellung von eurocheque-Karten hinzuweisen.

Auch habe ich die Praxis bemängelt, von Antragstellern, die ihr Postgirokonto nicht als Gehaltskonto führen wollen, Angaben zum Beruf zu verlangen. Diesem Bedenken hat der Bundesminister für Post und Telekommunikation inzwischen Rechnung getragen, so daß künftig auf Berufsangaben des Antragstellers verzichtet wird.

Darüber hinaus habe ich die Praxis der Bonitätsprüfung kritisiert, weil der Umfang der hierbei vom Antragsteller erhobenen Daten nicht eindeutig von Dienstanweisungen eingegrenzt wird. Das Verfahren empfinden offenbar auch Bedienstete des Postgiroamtes nicht als ausreichend präzise geregelt. Ich habe deshalb vorgeschlagen, in die Dienstanweisung eine enumerative Auflistung der vom Kunden zum Nachweis seiner Bonität vorzulegenden Unterlagen aufzunehmen und solche im Regelfall sensible Daten enthaltende Schriftstücke nach Einsichtnahme dem Kunden zurückzugeben. Auch diese Anregung hat der Bundesminister für Post und Telekommunikation bereits aufgegriffen, was ich ausdrücklich begrüße.

Die Kontrolle befaßte sich auch mit der Arbeit der Nachforschungsstelle des Postgiroamtes. Wie ich durch Akteneinsicht feststellen konnte, gibt diese Stelle auf Ersuchen Informationen aus dem Postgiroverhältnis (Kontobewegungen, Kontostaffeln) zur Aufklärung von Straftaten nicht nur an die Staatsanwaltschaft, sondern auch an Polizeibehörden weiter. Der Bundesminister für Post und Telekommunikation begründet diese Auskunftspraxis unter Hinweis auf § 161 Strafprozeßordnung, der gegenüber der Staatsanwaltschaft eine gesetzliche Auskunftspflicht im Sinne des § 6 Postgesetz festlege. Polizeibehörden könnten sich zwar nicht auf ein dem Recht der Staatsanwaltschaft gleichwertiges Auskunftsrecht berufen, ihre Anfragen dürften jedoch nicht generell unter Hinweis auf §§ 99, 100 StPO, wonach Beschlagnahmen dem Gericht und der Staatsanwaltschaft vorbehalten sind, zurückgewiesen werden. Dieser Rechtsauffassung habe ich widersprochen, weil für eine generelle Auskunftspflicht gegenüber Polizeibehörden eine gesetzliche Grundlage nicht existiert. Eine solche ist aber nach der klaren Regelung des § 6 PostG Voraussetzung für Auskünfte über Postgiro- und Postsparguthaben. Meine Kritik hat der Bundesminister für Post und Telekommunikation insoweit berücksichtigt, als er angekündigt hat, seinen der Auskunftspraxis der Postgiroämter zugrunde liegenden Erlaß zu präzisieren. Danach ist eine Klarstellung zu erwarten, wonach gemäß § 161 Strafprozeßordnung nur gegenüber der Staatsanwaltschaft und den von ihr *beauftragten* Polizeibehörden eine gesetzliche Auskunftspflicht besteht.

7.9 Sperrdatei im Postgirodienst

In meinem Zehnten Tätigkeitsbericht (S. 42f.) habe ich über die datenschutzrechtliche Problematik der sogenannten Sperrdatei berichtet. Dabei habe ich darauf hingewiesen, daß für diese Datei, in die ehemalige Postkunden, die nicht mehr zum Postgirodienst zugelassen sind, aufgenommen werden, eine normenklare Rechtsgrundlage fehlt. In Abstimmung mit mir hat der Bundesminister für Post und Telekommunikation nun mit § 9a Postgiroordnung die notwendige Rechtsgrundlage geschaffen. Die neue Vorschrift legt die Voraussetzung der Eintragung in die Sperrdatei fest und gibt Aufschluß über die Verwendung der Daten, den Kreis der Verwendungsberechtigten und die Speicherungsdauer. Damit ist eine datenschutzrechtlich einwandfreie Lösung gefunden worden.

7.10 Btx-Kontonummerauskunft im Postgirodienst

Der Bundesminister für Post und Telekommunikation kündigte im November 1988 durch eine Pressemitteilung die Einführung einer durch Bildschirmtext (Btx) zugänglichen Auskunft über Postgirokontonummern und -bezeichnungen (Name und Anschrift der Kontoinhaber) an, woraufhin mir zahlreiche Bürger ihre Bedenken gegenüber diesem erweiterten Informationsangebot zum Ausdruck brachten. Als Rechtsgrundlage für das neue Auskunftsverfahren sah die Deutsche Bundespost § 4 Abs. 3 der Postgiroordnung an: Danach können die Postgiroämter über die Kontonummer und die Kontobezeichnung Dritten Auskunft erteilen, soweit der Kontoinhaber nicht widersprochen hat.

Bei meiner Überprüfung des postinternen Pilotbetriebs habe ich datenschutzrechtliche Mängel des geplanten Auskunftsangebotes festgestellt: So konnte das Verfahren nicht sicherstellen, daß bei der Btx-Abfrage nur diejenigen personenbezogenen Informationen preisgegeben wurden, die auch im konventionellen Verfahren, d. h. bei der Einzelanfrage beim Postgiroamt, zulässigerweise erteilt worden wären. Das technische Konzept sah vielmehr vor, bei Namensgleichheit von Kontoinhabern sämtliche diesem Namen zugeordneten Kontonummern und Kontobezeichnungen dem anfragenden Btx-Kunden zur Auswahl anzubieten. Ein derartiges „Komplettangebot" personenbezogener Informationen wäre jedoch einer teilweisen Wiedereinführung eines öffentlichen Teilnehmerverzeichnisses der Postgirokunden gleichgekommen. Solche Teilnehmerverzeichnisse wurden nach 1976 nicht mehr veröffentlicht, weil sie datenschutzrechtlich nicht zulässig waren. Ich habe deshalb den Bundesminister für Post und Telekommunikation gebeten, die technischen Vorkehrungen zu schaffen, um den Umfang der per Btx übermittelten Daten auf das notwendige Maß im Sinne einer automatisierten Einzelauskunft zu reduzieren. Ein datenschutzgerechtes Btx-Suchsystem hätte insbesondere auch sicherstellen müssen, daß Daten von Postgirokunden, die nach § 4 Abs. 3 Postgiroordnung der Kontonummermitteilung an Dritte widersprochen haben, nicht mehr abrufbar sind.

Der Bundesminister sah sich jedoch außerstande, diese datenschutzrechtlichen Forderungen zu erfüllen. Ich begrüße daher seine Entscheidung, das Vorhaben Btx-Kontonummerauskunft im Postgirodienst nicht weiterzuverfolgen.

7.11 Weitergabe der Anschrift von Postfachinhabern

Ein Bürger, der ein Postfach besitzt, hat sich an mich gewandt, weil die Deutsche Bundespost seine Anschrift einem anfragenden Dritten mitgeteilt hatte.

Der Bundesminister für Post und Telekommunikation sieht für diese Auskunftspraxis in den allgemeinen Übermittlungsregelungen des § 11 BDSG eine hinreichende Rechtsgrundlage. Er vertritt die Auffassung, daß die Einrichtung eines Postfaches nicht der Geheimhaltung der Anschrift seines Inhabers dienen könne. Auskünfte über die Anschrift von Postfachabholern fielen auch nicht unter das Postgeheimnis.

Die Rechtsauffassung des Bundesministers für Post und Telekommunikation teile ich nicht. § 11 BDSG vermag die Praxis der Deutschen Bundespost, anfragenden Dritten die Anschrift von Postfachinhabern mitzuteilen, nicht ausreichend zu stützen. Abgesehen von der schwierig zu entscheidenden Frage, welche Anfragegründe ausreichend sein sollen, um von einem glaubhaft gemachten berechtigten Interesse an der Auskunft sprechen zu können, kann nicht allgemein davon ausgegangen werden, daß schutzwürdige Belange des Postfachinhabers durch Weitergabe seiner Anschrift nicht betroffen sind: Zahlreiche Postkunden, die von der Möglichkeit, Postsendungen beim Postamt abholen zu können, Gebrauch machen, wählen diese Zustellungsart, um ihre Anschrift nicht preisgeben zu müssen. Postfachinhaber brauchen infolge Fehlens einer entsprechenden rechtlichen Regelung auch nicht damit zu rechnen, daß das Postamt ihre Anschrift Dritten mitteilt.

Ich habe daher den Bundesminister für Post und Telekommunikation aufgefordert, sofern er seine Praxis, Anschriften von Postfachinhabern weiterzugeben, aufrechterhalten wolle, hierfür eine normenklare Rechtsgrundlage zu schaffen, die zugleich auch das Widerspruchsrecht des Postfachinhabers gegen die Anschriftenweitergabe normieren müßte. Eine vergleichbare Regelung enthält — aufgrund meiner Anregungen — bereits § 38 Postordnung im Zusammenhang mit der Anschriftenprüfung (s. 7.6).

8 Verkehrswesen

Schwerpunkte meiner Tätigkeit auf dem Gebiet des Verkehrswesens waren im Berichtsjahr

— Probleme im Zusammenhang mit dem Zentralen Verkehrsinformationssystem (ZEVIS), insbesondere zum Umfang und zur Auswertbarkeit von ZEVIS-Protokollierungen (s. 8.1) sowie Kontrollen und Beratungen in diesen Fragen (s. 8.1.1 und 8.1.2),

— Festlegung der Voraussetzungen, unter denen aus datenschutzrechtlicher Sicht unbedenkliche Übermittlungen von Kfz-Zulassungsdaten an Kfz-Hersteller und Kfz-Importeure ermöglicht werden können (s. 8.3),

— Kontrolle und Beratung der Deutschen Bundesbahn, insbesondere zu der Problematik der Speicherung von Schwarzfahrten strafunmündiger Kinder,

— Erhebung und Speicherung personenbezogener Daten im Rahmen der Vorbereitung und Abwicklung des Flugverkehrs (s. 8.6.1).

Die personelle Situation meiner Dienststelle war auch in diesem Berichtsjahr ursächlich dafür, daß auf dem Gebiet des Verkehrswesens drei vorgesehene Kontrollen (ZEVIS-Abrufe durch den BGS und Zoll, eine Wasser- und Schiffahrtsdirektion, Deutsches Hydrographisches Institut) nicht durchgeführt und die Kontrolle und Beratung der Bundesanstalt für Flugsicherung nicht abschließend bewertet werden konnten.

Erschwert wurde meine Arbeit darüber hinaus dadurch, daß der Bundesminister für Verkehr meine Dienststelle in Einzelfällen bei der Vorbereitung von Gesetzen und Verordnungen nicht ausreichend oder gar nicht beteiligt hat. Erst durch meine Intervention beim Bundesrat wurden z. B. bei den Entwürfen einer Gefahrgutbeauftragtenverordnung und der 2. Straßen-Gefahrgutänderungsverordnung datenschutzrechtlich unklare Regelungen geändert. Bei der Vorbereitung des Entwurfs eines Straßenbenutzungsgebührengesetzes wurde ich nach Abgabe einer Stellungnahme zu einem Vorentwurf nicht mehr beteiligt. Erst über die Presse erfuhr ich von der Kabinettsentscheidung über den Gesetzentwurf. Ich habe dem Bundesminister für Verkehr gleichwohl meine Vorschläge für normenklare Regelungen zu der Führung der in diesem Zusammenhang zu schaffenden Register unterbreitet. Die unzureichende Beteiligung meiner Dienststelle widerspricht dem mehrfach zum Ausdruck gebrachten Willen des Deutschen Bundestages (BT-Drucksachen 9/1623 und 10/6583); darauf habe ich den Bundesminister für Verkehr hingewiesen.

8.1 Zentrales Verkehrsinformationssystem (ZEVIS)

Zur Vorbereitung des dem Deutschen Bundestag zu Beginn des Jahres 1991 vorzulegenden ZEVIS-Erfahrungsberichtes (11. TB S. 37 — vgl. 7.1 —) habe ich mich im Berichtszeitraum verstärkt mit den Problemen des Aufbaus, des Betriebs und der Nutzung des Zentralen Verkehrsinformationssystems befaßt. Das Kraftfahrt-Bundesamt hat inzwischen mit meiner Unterstützung eine Verbesserung des Abrufverfahrens und seiner organisatorischen Voraussetzungen erzielt. Die hierbei immer noch festgestellten Defizite und Mängel, die von grundsätzlicher Bedeutung sind, werden nachfolgend dargestellt; eine abschließende Bewertung kann erst nach Eingang der aus Zeitgründen noch nicht vorliegenden Stellungnahme des Bundesministers für Verkehr erfolgen. Im nächsten Berichtsjahr wird es darauf ankommen, die gewonnenen Erkenntnisse durch weitere Kontrollen noch einmal zu

überprüfen sowie die Erfahrungen der Landesbeauftragten für den Datenschutz aufzubereiten, die unter Berücksichtigung des von einer Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Fahrzeugregister-Informationskonzeptes gewonnen wurden.

8.1.1 Probleme des Aufbaus und des Betriebs

Online-Anschlüsse

Anträge auf Vergabe von ZEVIS-Berechtigungen gehen dem Kraftfahrt-Bundesamt (KBA) in der Regel über die jeweils zuständigen Landeskriminalämter (ggf. über das Bundeskriminalamt) nach deren Prüfung auf technische Realisierungsmöglichkeit zu. Vor Schaltung der Berechtigungen werden die dienstaufsichtsführenden Behörden dieser Dienststellen um Abgabe einer Erklärung dahingehend gebeten, daß die Dienststellen Daten aus dem Zentralen Verkehrsinformationssystem nur zu den gesetzmäßigen Zwekken nach § 36 des Straßenverkehrsgesetzes (StVG) und § 12 Abs. 1 Satz 2 der Fahrzeugregisterverordnung (FRV) beim KBA abrufen. Nach Auffassung des KBA ist hierdurch sichergestellt, daß Abrufe nur von den berechtigten Dienststellen zu den gesetzlich vorgesehenen Zwecken erfolgen. Gleichwohl habe ich festgestellt, daß das KBA aufgrund des Antrages eines Landeskriminalamtes (LKA) eine ZEVIS-Berechtigung für eine nicht abrufberechtigte Stelle vergeben hatte. Obwohl dem Antrag ein Mißverständnis zugrunde lag und Abrufe wegen der vom LKA unterlassenen Weiterleitung der ZEVIS-Kennung nicht erfolgten, bestätigt dieses Vorkommnis meine Auffassung, daß die beim KBA als der speichernden Stelle liegende Verantwortung für die Gewährung des ZEVIS-Zugriffs mit besonderer Sorgfalt wahrgenommen werden muß. Ich habe das KBA daher gebeten, die Abrufberechtigung jeder Stelle, deren Anschluß beantragt wird, auf ihre Plausibilität vor Schaltung einer ZEVIS-Berechtigung zu prüfen, soweit erforderlich auch unter Einschaltung der dienstaufsichtsführenden Behörden.

Kennungsvergabe

Die Änderung der ZEVIS-Kennungen nach § 13 Abs. 1 FRV erfolgt in einem Turnus von jeweils 18 Monaten. Ich habe dem KBA aus Gründen der DV-Sicherheit vorgeschlagen, diesen Rhythmus auf sechs Monate bis zu einem Jahr zu verkürzen oder eine Selbstvergabe durch die abrufberechtigten Dienststellen in kürzeren Zeitabständen einzuführen. Das Amt hat dies unter Hinweis auf die Rechtslage und die personellen Engpässe abgelehnt. Ich bedauere diese Entscheidung, zumal das geltende Recht eine Verkürzung ohne weiteres zuläßt.

Die Entwicklung der Technik und die erkennbar steigende Tendenz bei der Computerkriminalität machen es erforderlich, mit ZEVIS-Kennungen in Zukunft noch sorgfältiger umzugehen, um unberechtigte Abrufe zu verhindern. Dieses Problem wird wahrscheinlich durch den zukünftig verstärkten Einsatz von Funkterminals bei der Polizei noch an Bedeutung gewinnen. Dem KBA als übermittelnde Stelle obliegt die Verpflichtung, dafür Sorge zu tragen, daß nicht durch technische Manipulationen unberechtigte Datenübermittlungen erfolgen können; zumindest sollten sie soweit irgend möglich erschwert werden. Ich habe dem KBA daher empfohlen, die dienstaufsichtsführenden Behörden auf die Problematik des möglichen Mißbrauchs von ZEVIS-Abrufen hinzuweisen und zu fordern, daß zumindest die Kennungen von Funkterminals kryptographisch zu verschlüsseln sind. Über etwaige darüber hinaus gehende sinnvolle Maßnahmen zur Sicherung gegen unberechtigte Abrufe werde ich mit dem KBA weitere Gespräche führen.

Fahrerlaubnisabfragen

Abrufe aus dem Verkehrszentralregister über entzogene Fahrerlaubnisse (*F-Anfragen) sind nach § 30a des Straßenverkehrsgesetzes nur an die Fahrerlaubnisbehörden und die Polizeien der Länder sowie an die mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs beauftragten Dienststellen des Bundes zwecks Prüfung der Berechtigung zum Führen eines Kraftfahrzeuges erlaubt. Ich habe jedoch festgestellt, daß das Bundeskriminalamt in der Zeit vom Oktober 1987 bis Juli 1989 insgesamt 201 *F-Abrufe — nach Angaben des BKA überwiegend zu Schulungszwecken — durchgeführt hat. Dies war nur möglich, weil das KBA teils bestehende Anschlüsse des BKA nicht rechtzeitig abgeschaltet, teils neue Anschlüsse mit der unzulässigen Abrufberechtigung eingerichtet hat.

Das KBA hat eingeräumt, daß die faktische Möglichkeit zur Durchführung von *F-Anfragen durch das BKA noch bis Ende des Jahres 1988 bestanden hat und daß die zu Beginn des Jahres 1989 für das BKA geschalteten drei neuen Anschlüsse noch mit der *F-Abrufberechtigung versehen waren. Die rechtzeitige Abschaltung dieser Abrufmöglichkeit sei aus Versehen unterblieben.

Diese gegen § 30a des Straßenverkehrsgesetzes verstoßende Datenübermittlungen habe ich gemäß § 20 Abs. 1 BDSG gegenüber dem Bundesminister für Verkehr und dem Bundesminister des Innern (vgl. auch 8.1.2 dieses Berichts) beanstandet.

Auskünfte über stillgelegte Fahrzeuge

Es sind Zweifel entstanden, ob § 36 Abs. 2 in Verbindung mit § 35 Abs. 1 StVG eine Halterauskunft rechtfertigt, wenn Anfragen an ZEVIS mit der Fahrzeugidentifizierungsnummer auf Fahrzeuge treffen, die für den öffentlichen Straßenverkehr nicht mehr zugelassen sind. In solchen Fällen werden nämlich personenbezogene Daten des bisherigen Halters übermittelt, ohne daß es sich um Halterdaten in bezug auf ein zugelassenes Fahrzeug im Sinne von § 33 Abs. 1 Nr. 2 StVG handelt. Ich werde dieses Problem mit dem Bundesminister für Verkehr erörtern.

Speicherung von roten Kennzeichen zur wiederkehrenden Verwendung

Die Speicherung entzogener oder zurückgegebener roter Kennzeichen zur wiederkehrenden Verwendung wurde mit dem KBA vor allem unter dem Gesichtspunkt ihrer Notwendigkeit diskutiert. Es bestehen Zweifel, ob es sich bei solchen Kennzeichen noch um Fahrzeugdaten im Sinne von § 33 Abs. 1 Nr. 1 StVG handelt und ob eine Speicherung dieser Daten in den Fahrzeugregistern zulässig ist. Auch diese Rechtsfrage werde ich mit dem Bundesminister für Verkehr noch erörtern.

*Realisierung der *P-Anfrage*

Das Konzept für die Realisierung der sog. *P-Anfrage (Abruf von Fahrzeug- und Halterdaten unter Verwendung von Personalien) geht davon aus, daß der Suchlauf beim KBA mit den in § 12 Abs. 1 Nr. 3 der Fahrzeugregisterverordnung als zulässig genannten Anfragedaten wegen nicht selten auftretender Namensgleichheit eine eindeutige Zuordnung zu einem Halter oft nicht ermöglicht. Das KBA hatte daher vorgeschlagen, zur Reduzierung von Mehrfachauskünften zusätzliche fahrzeugbezogene Eingrenzungskriterien vorzusehen.

Ich habe den Bundesminister für Verkehr darauf hingewiesen, daß nach § 36 Abs. 4 StVG sämtliche online-Abrufe sich nur auf ein bestimmtes Fahrzeug oder einen bestimmten Halter richten dürfen. Läßt sich eine eindeutige Zuordnung zum Halter eines Fahrzeugs nicht erreichen, so darf nach der gegenwärtigen Rechtslage der Umfang der Daten, mit denen Anfragen unter Verwendung von Personalien durchgeführt werden, nicht über den in § 12 Abs. 1 Nr. 3 der Fahrzeugregisterverordnung ausdrücklich genannten Umfang hinaus erweitert werden. Die in dieser Vorschrift enthaltenen Merkmale stellen nämlich eine abschließende Aufzählung der Personendaten dar, mit deren Hilfe ein Abruf durchgeführt werden darf.

Der Bundesminister für Verkehr hat aufgrund eines mit dem Bundesminister des Innern und mir geführten Gesprächs nunmehr vorgeschlagen, zur besseren Eingrenzung der gesuchten Person entsprechend der Anfrage mit einem Teil des Kennzeichens (*A-Anfrage) eine Voranfrage zu eröffnen und darüber hinaus zur Eingrenzung des technischen Suchlaufs die Erweiterung der Abrufdaten um die Anschrift vorzusehen. Der Bundesminister für Verkehr ist bereit, die Fahrzeugregisterverordnung noch im Laufe des Jahres 1990 entsprechend zu ergänzen.

Gegen diese Änderung der Verordnung habe ich keine Bedenken. Ich habe dem Bundesminister für Verkehr meine Beratung bei der Ausgestaltung der neuen Abfrageart und der Festlegung des Auskunftsumfangs angeboten.

Mit dem Bundesminister für Verkehr und dem Bundesminister des Innern wurde Einigung über eine Vorabregelung bis zur Änderung der Fahrzeugregisterverordnung dahingehend erzielt, daß zur Eingrenzung des Suchlaufs beim KBA die Abfragedaten bei Anfragen unter Verwendung von Personalien um das Unterscheidungszeichen des Kfz-Kennzeichens und die Länderschlüsselnummer als Hilfsmerkmale für die später vorzusehende Anschrift erweitert werden dürfen. Darüber hinaus hat das KBA sicherzustellen, daß bei trotzdem noch auftretenden Mehrfachauskünften nur Datensätze übermittelt werden, die höchstens fünf verschiedenen Personen zuzuordnen sind. Unter diesen Voraussetzungen konnte die *P-Anfrage im Januar 1990 realisiert werden.

ZEVIS-Protokollierungen

Ich habe dem KBA Vorschläge für eine Änderung der ZEVIS-Protokollierung sowie für eine programmgesteuerte Minimalauswertung der ZEVIS-Protokolle gemacht. Ich messe dieser Initiative im Hinblick auf deren Vorbildfunktion für die automatisierten örtlichen Fahrzeugregister und der damit erreichbaren Vergleichbarkeit von Auswertungen über Abrufe aus den Fahrzeugregistern große Bedeutung bei.

Ich habe festgestellt, daß das KBA bei der Auswahlprotokollierung gemäß § 36 Abs. 7 StVG inzwischen eine Plausibilitätsprüfung hinsichtlich der Angabe der zulässigen Schlüsselzahlen und der gesetzlich geforderten Zusatzangaben durchführt. Es ist jedoch noch immer möglich, unsinnige oder falsche Zusatzangaben zu machen, ohne daß das System den Abruf abbricht; dies ist auch der Fall, wenn die Zusatzangabe in keinem inneren Zusammenhang mit den Schlüsselzahlen steht. Ich habe das KBA darauf hingewiesen, daß die Plausibilität der Zusatzangaben im Rahmen der Auswahlprotokollierung — zumindest stichprobenweise — zu kontrollieren ist.

8.1.2 Nutzung durch das Bundeskriminalamt

Bei meiner Kontrolle der ZEVIS-Nutzung durch das Bundeskriminalamt habe ich festgestellt, daß das BKA keine generelle Weisung über Zulässigkeit, Art, Umfang und Dokumentation von ZEVIS-Abrufen erlassen hat. Die Organisationsstruktur des BKA führt bei ZEVIS-Anfragen dazu, daß die fachliche Verantwortung für Abrufe oft nicht feststellbar ist, die Dokumentation der ZEVIS-Abrufe nicht nach einem einheitlichen Verfahren geschieht und die für die Abrufe maßgeblichen Gründe nicht ausreichend dokumentiert sind. Ich habe dem BKA daher empfohlen, eine Handlungsanweisung der oben beschriebenen Art zu erlassen sowie Anleitungen zur Dokumentation zu geben.

Das BKA bestreitet die Notwendigkeit zum Erlaß einer generellen Weisung, da nach seiner Auffassung die polizeilichen/strafverfolgungsmäßigen Belange ausschlaggebend für eine Nutzung des Online-Systems seien. Im Gegensatz dazu halte ich gerade wegen der unterschiedlichen Aufgabenstellungen der einzelnen Abteilungen eine zentrale Weisung zur Gewährleistung möglichst einheitlicher Verfahren bei ZEVIS-Abrufen und eine ausreichende Dokumentation für erforderlich.

Innerhalb des BKA fanden bisher Kontrollen der ZEVIS-Abrufe nicht statt. Dies ist nach meiner Überzeugung mit ursächlich für folgende von mir festgestellte, mit dem Straßenverkehrsgesetz unvereinbare Abrufpraktiken:

— Insgesamt 201 automatisierte Abrufe aus dem Verkehrszentralregister über entzogene Fahrerlaubnisse (*F-Anfrage) in der Zeit vom Oktober 1987 bis Juli 1989. Nach § 30a des Straßenverkehrsgesetzes ist diese Abfrage nur den Fahrerlaubnisbehörden und den Polizeien der Länder sowie den mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs beauftragten Dienststellen des Bundes zwecks Prüfung der Berechtigung zum Führen eines Kraftfahrzeuges — also nicht dem BKA — erlaubt.

— Automatisierte Abrufe aus dem zentralen Fahrzeugregister zur Ermittlung der Unfallgegner von BKA-Dienstfahrzeugen, um zivilrechtliche (Schadensersatz-)Ansprüche verfolgen zu können.

  Für diesen Zweck erlaubt § 36 StVG keine Online-Abfrage.

Die gegen § 30a und § 36 StVG verstoßenden Datenübermittlungen des Kraftfahrt-Bundesamtes an das Bundeskriminalamt habe ich gegenüber dem Bundesminister für Verkehr gemäß § 20 Abs. 1 BDSG beanstandet (s. 8.1.1 — Fahrerlaubnisabfragen).

Die Verantwortung für die Übermittlung personenbezogener Daten durch Abruf im automatisierten Verfahren trifft gleichermaßen auch die abrufende Stelle. Das BKA hatte aber nichts unternommen, um derartige unzulässige Datenübermittlungen durch die abrufberechtigten Stellen seines Hauses zu verhindern. Nicht zuletzt dadurch wurden rechtswidrige Datenabrufe der beschriebenen Art ermöglicht. Dieses habe ich gegenüber dem Bundesminister des Innern gemäß § 20 Abs. 1 BDSG beanstandet.

Das BKA hat geltend gemacht, die Abrufe aus dem Verkehrszentralregister über entzogene Fahrerlaubnisse hätte Schulungszwecken gedient und bei den automatisierten Abrufen aus dem Zentralen Fahrzeugregister seien keine Daten übermittelt worden, die dem BKA bei konventioneller Anfrage hätten vorenthalten werden müssen. Das BKA hat die Rechtswidrigkeit der dargestellten Verfahren eingeräumt, aber die Auffassung vertreten, es lägen allenfalls unbedeutende Verstöße vor, die keine Beanstandung rechtfertigten. Diese Auffassung teile ich nicht. Die Aufrechterhaltung dieser Online-Anschlüsse und deren Nutzung über Jahre hinweg gegen klare gesetzliche Vorschriften bewerte ich vielmehr als gravierenden datenschutzrechtlichen Verstoß.

Die in den §§ 35 und 36 StVG vorgeschriebenen Protokollierungen der ZEVIS-Abrufe sollten nach dem Willen des Gesetzgebers ausreichen, um eine effektive Datenschutzkontrolle zu gewährleisten. Ich habe jedoch festgestellt, daß die durch die Organisationsstruktur des BKA bedingte Abrufpraxis eine derartige Kontrolle tatsächlich nicht ermöglicht. Die gesetzlich vorgesehenen Protokollierungen reichen außerdem nicht aus, damit das BKA seiner Verantwortung für die Rechtmäßigkeit der von ihm ausgehenden ZEVIS-Abrufe gerecht wird und seine Verpflichtung zur Gewährleistung des Datenschutzes im Sinne des § 6 BDSG erfüllt. Ich habe dem BKA daher vorgeschlagen, ergänzend eine manuelle Aufzeichnung der ZEVIS-Abrufe vorzunehmen, aus der sich insbesondere der für den Abruf fachlich Verantwortliche ergibt. Das BKA hat dieser Auffassung unter Hinweis auf die Regelungen des StVG, nach denen dies nicht verlangt wird, widersprochen. Ich werde das Problem mit dem BKA weiter erörtern. Sollte sich dabei keine Lösung ergeben, ist eine Ergänzung des geltenden Rechts unerläßlich, um eine wirksame Kontrolle der Abrufe zu ermöglichen.

8.2 Verkehrszentralregister

8.2.1 Stand der Gesetzgebung

Ich habe bereits mehrfach auf die Notwendigkeit normenklarer gesetzlicher Regelungen für die Datenverarbeitung des Verkehrszentralregisters hingewiesen (9. TB S. 36, 10. TB S. 46, 11. TB S. 94 Nr. 22). Der Bundesminister für Verkehr hat dies bereits aufgrund meiner im Jahre 1984 ausgesprochenen Beanstandung anerkannt. Gleichwohl liegt auch jetzt — fünf Jahre nachdem das Regelungsdefizit erkannt wurde — noch immer kein entsprechender Gesetzentwurf vor. Die vom Bundesminister für Verkehr im Vorgriff auf die noch ausstehende Novellierung zum 1. August 1989 angeordnete Reduzierung der Datenübermittlung (s. 8.2.2) ist zwar zu begrüßen, für sich allein aber nicht geeignet, bestehende Bedenken auszuräumen.

Die Prüfung der Frage einer Kooperation zwischen Bundeszentralregister und Verkehrszentralregister ist nach Mitteilung des Bundesministers für Verkehr noch nicht abgeschlossen, soll jedoch im Zusammenhang mit der Novellierung der Vorschriften für das Verkehrszentralregister entschieden werden.

8.2.2 Auskunftserteilung nach § 30 StVG (Vollauskunft)

Über erste Überlegungen des Bundesministers für Verkehr für Teilauskunftsregelungen im Rahmen der Novellierung der Vorschriften über das Verkehrszentralregister habe ich berichtet (10. TB S. 46). Inzwischen hat der Bundesminister für Verkehr mitgeteilt, daß seit dem 1. August 1989 im Vorgriff auf die Novellierung folgende Regelungen eingeführt sind:

— Bei Anfragen für die Ausstellung von Ersatzführerscheinen und für die Ausgabe von roten Kennzeichen zur wiederkehrenden Verwendung wird nur noch eine Teilauskunft erteilt.

— Für Erteilung, Rücknahme und Widerruf der Anerkennung als Sehteststelle und für die Anerkennung der Eignung einer „anderen Stelle" für die Unterweisung in Sofortmaßnahmen am Unfallort oder die Ausbildung in Erster Hilfe wird auf die Vorlage einer Auskunft aus dem Verkehrszentralregister ganz verzichtet.

— In den übrigen Fällen wird wie bisher Vollauskunft erteilt.

Für die Novellierung der Vorschriften über das Verkehrszentralregister gehen die Überlegungen des Bundesministers für Verkehr dahin, bei der Verfolgung von Ordnungswidrigkeiten nach anderen Gesetzen als dem Straßenverkehrsgesetz weitgehend auf Auskünfte aus dem Verkehrszentralregister zu verzichten. Für Verwaltungsmaßnahmen sollen dagegen im wesentlichen Auskünfte für die gleichen Zwecke wie bisher gegeben werden, wobei der Inhalt der Auskünfte sich nach einem abgestuften System an der Art und Weise der Datennutzung ausrichten soll. Die in diesen Vorstellungen enthaltenen Auskunftseinschränkungen gehen in die richtige Richtung.

Ich hoffe, daß der Gesetzentwurf nunmehr in Kürze erstellt wird.

8.3 Übermittlung von Kfz-Zulassungsdaten an die Automobilindustrie

Über die datenschutzrechtlichen Probleme, die nach Inkrafttreten des Gesetzes zur Änderung des Straßenverkehrsgesetzes vom 28. Januar 1987 im Zusammenhang mit der Übermittlung von Kfz-Zulassungsdaten durch das Kraftfahrt-Bundesamt an die Automobilhersteller und -importeure entstanden waren, sowie über Alternativen zur Lösung dieser Probleme habe ich berichtet (10. TB S. 46f., 11. TB S. 38).

Die Datenübermittlungen wurden inzwischen zum Teil wieder aufgenommen, nachdem mit einzelnen Firmen Einigungen über datenschutzrechtlich gangbare Lösungen erzielt werden konnten. Unter anderem wird bei diesen wie folgt verfahren:

Die überwiegende Zahl der Importeure erbittet bei Veräußerung eines Kfz die Zustimmung ihrer Kunden zur Übermittlung ihrer Zulassungsdaten (u. a. vollständige Fahrzeugidentifizierungs-Nummer) an die Importeure auf dem Wege über die Händler und das KBA. Der Wortlaut der dabei verwendeten Einwilligungserklärung ist mit mir abgestimmt worden. Das KBA sollte als Vertragspartner der Importeure das Vorliegen dieser Einwilligungserklärung in Einzelfällen — zumindest stichprobenweise — kontrollieren. Ich werde auch in Zukunft prüfen, ob bei nicht erteilter Zustimmung die Datenübermittlung auch tatsächlich unterbleibt und dieses Ergebnis nicht durch anderweitige Verpflichtungen der Händler gegenüber den Importeuren unterlaufen werden kann.

Andere Importeure und einige Hersteller verzichten auf die Übermittlung von Kundendaten durch ihre Händler. Wie ich in meinen 10. TB S.47 dargelegt habe, ist die Automobilindustrie nur mit Hilfe dieser Informationen in der Lage, den Halter eines neu zugelassenen Fahrzeugs festzustellen. Die praktizierte Übermittlung der teilanonymisierten Zulassungsdaten (u. a. gekürzte Fahrzeugidentifizierungs-Nummer) durch das KBA stellt sich damit als eine Übermittlung anonymisierter Daten im Sinne des § 45 StVG dar, der § 35 Abs.2 Nr.1 StVG nicht entgegensteht.

Andere Hersteller führen die Verarbeitung der Kundendaten in Zukunft ausschließlich im Auftrag und für Zwecke ihrer Händler durch. Damit verfügen sie über keinerlei (eigene) Kundendaten, so daß auch nach den unter meiner Mitwirkung erarbeiteten und mit den Händlern abgeschlossenen Zusatzvereinbarungen zum Händlervertrag eine Verknüpfung dieser Daten mit den teilanonymisierten Zulassungsdaten und damit die Herstellung eines Personenbezuges nicht mehr in Betracht kommt. Die Übermittlung der teilanonymisierten Zulassungsdaten durch das KBA an diese Hersteller stellt daher eine zulässige Übermittlung anonymisierter Daten im Sinne von § 45 StVG dar.

8.4 Fahrerlaubnisdaten

Über die notwendige Verbesserung der bisher unzureichenden gesetzlichen Regelung für die Erhebung und Verarbeitung von Fahrerlaubnisdaten habe ich berichtet (10. TB S. 47 f.) und die Bereitschaft des Bundesministers für Verkehr zu einer entsprechenden Novellierung des Straßenverkehrsgesetzes begrüßt (11. TB S. 94 Nr. 23).

Im Berichtsjahr wurde die Dringlichkeit dieser Maßnahme deutlich, da im Zuge der fortschreitenden Automatisierung die Fahrerlaubnisbehörden und Sonderfahrerlaubnisbehörden (z. B. Deutsche Bundespost) verstärkt dazu übergehen, noch mehr Informationen als bisher zu speichern und diese Daten auch für andere Zwecke zu nutzen. Ich habe erhebliche Zweifel, ob eine Datenspeicherung in diesem Umfang für die Erfüllung der Aufgaben dieser Behörden tatsächlich erforderlich ist. Die Novellierung des Straßenverkehrsgesetzes muß dies möglichst rasch klären. Ein entsprechender Gesetzentwurf ist mir bisher allerdings nicht bekannt geworden, obwohl ein solcher bereits im Jahre 1988 angekündigt worden war.

8.5 Luftfahrt

Die aufgrund meiner in den Jahren 1984 und 1986 beim Luftfahrt-Bundesamt durchgeführten Kontrollen festgestellten Regelungsdefizite (7. TB S. 36, 9. TB S. 36) wurden auch im Berichtsjahr noch nicht behoben. Zusätzliche Rechtsfragen haben sich in bezug auf die Erhebung und Verarbeitung personenbezogener Daten im Zusammenhang mit der Vorbereitung und Abwicklung des Flugverkehrs sowie der Zulässigkeit der Herstellung, Freigabe, Veräußerung und Aufbewahrung von Luftbildaufnahmen durch gewerbliche Luftbildunternehmen ergeben.

8.5.1 Gesetzliche Regelungen auf dem Gebiet der Luftfahrt

Im Elften Tätigkeitsbericht (S. 39f.) habe ich an die Notwendigkeit erinnert, die Veröffentlichung von personenbezogenen Daten der Eigentümer von Luftfahrzeugen, die im Rahmen der Verkehrszulassung erhoben und in der Luftfahrzeugrolle eingetragen sind, auf eine ausreichende gesetzliche Grundlage zu

stellen. Die mit dem Bundesminister für Verkehr in diesem Zusammenhang erörterten Änderungen des Gesetzes über das Luftfahrt-Bundesamt und der Luftverkehrszulassungsordnung sind noch immer nicht über das Entwurfsstadium hinausgekommen.

Der Bundesminister für Verkehr hatte die Notwendigkeit der von mir bereits im Jahre 1984 geforderten gesetzlichen Regelung für die Führung der Datensammlung für Luftfahrer grundsätzlich anerkannt. Leider sind mir auch in diesem Berichtsjahr keine Vorschläge zur Verbesserung der Rechtsgrundlagen bekannt geworden. Der Bundesminister für Verkehr hat lediglich mitgeteilt, daß er „weiterhin bemüht ist, in notwendiger Übereinstimmung mit den beteiligten Landesbehörden den Entwurf verbesserter Rechtsvorschriften zu erstellen".

Zu der von mir geforderten ausreichenden gesetzlichen Grundlage für die Erhebung, Speicherung und Übermittlung von personenbezogenen Informationen bei der Wahrnehmung der Aufgaben der Flugunfalluntersuchungsstelle des Luftfahrt-Bundesamtes hat der Bundesminister für Verkehr mitgeteilt, daß inzwischen Entwürfe einer Verordnung über die Untersuchung von Flugunfällen oder Störungen beim Betrieb von Luftfahrzeugen (LuftUV) sowie einer ergänzenden Verwaltungsvorschrift erstellt worden seien, die jedoch noch innerhalb des Ministeriums sowie mit der Flugunfalluntersuchungsstelle beim Luftfahrt-Bundesamt abgestimmt werden müßten.

Aufgrund einer Eingabe bin ich darauf aufmerksam geworden, daß die Flugplatzhalter im Rahmen ihrer Verpflichtung zur Führung eines Hauptflugbuches oder andere von ihnen beauftragte Stellen personenbezogene Daten der Halter von Luftfahrzeugen und von Luftfahrzeugführern speichern, ohne daß es hierfür ausreichende Rechtsnormen gibt. Der Bundesminister für Verkehr hat anerkannt, daß die Rechtslage durch Änderungen der Luftverkehrs-Zulassungsordnung und der Luftverkehrsordnung präzisiert werden sollte. Bis zum Erlaß dieser Novellen hält er § 6 des Luftverkehrsgesetzes (Festlegung von Auflagen im Rahmen der Erteilung der Genehmigungen zum Anlegen und zum Betrieb von Flugplätzen) im Hinblick auf die durch die Flughafenbenutzungs-Ordnung privatrechtlich geregelten Verpflichtungen des Luftfahrzeugführers für ausreichend.

Ich habe den Bundesminister für Verkehr gebeten, mich bei entsprechenden Entwürfen rechtzeitig zu beteiligen.

8.5.2 Luftbildaufnahmen

Der von der Bundesregierung eingebrachte Entwurf eines Gesetzes zur Novellierung des Bundesdatenschutzgesetzes begrenzt die Datenschutzkontrolle auf in Dateien gespeicherte personenbezogene Daten. Auch dadurch wurde die Diskussion darüber verstärkt, ob und gegebenenfalls in welcher Weise das Recht des einzelnen auf informationelle Selbstbestimmung durch Kenntnisnahme personenbezogener Informationen verletzt sein kann, auch ohne daß diese in Dateien gespeichert sind. Ein Aspekt dieser Diskussion ist auch die Herstellung, Aufbereitung und Verbreitung von Bildern. Ich habe bereits vor Jahren (8. TB S. 26) die Auffassung vertreten, daß der gesetzliche Datenschutz künftig auf Bilder ausgedehnt werden muß.

Zu diesem Problemkreis gehört auch die Herstellung, Freigabe, Veräußerung und Aufbewahrung von Luftbildaufnahmen durch gewerbliche Luftbildunternehmen. Ich werde mit dem Bundesminister für Verkehr erörtern, ob im Rahmen der Erteilung einer Erlaubnis zur Anfertigung und Verbreitung von Luftbildaufnahmen nach § 27 Abs. 2 des Luftverkehrsgesetzes Gesichtspunkte der Beeinträchtigung des Persönlichkeitsrechts berücksichtigt werden können und ob zu diesem Zweck die einschlägigen Vorschriften der Luftverkehrszulassungsordnung zu ergänzen sind.

8.6 Deutsche Bundesbahn

Über die aus meiner Sicht verbesserungswürdigen organisatorischen Regelungen zur Sicherstellung der datenschutzrechtlichen Verantwortung innerhalb der Deutschen Bundesbahn habe ich berichtet (10. TB S. 48). Die von der Deutschen Bundesbahn bereits im letzten Berichtsjahr angekündigte Untersuchung ihres Organisationsbereichs, inwieweit Verbesserungen bei der Anwendung und Überwachung der datenschutzrechtlichen Vorschriften möglich sind (11. TB S. 94 Nr. 24), liegen mir noch nicht vor. Ich habe die Deutsche Bundesbahn gebeten, mir vor Herausgabe neuer interner Datenschutzvorschriften Gelegenheit zur Stellungnahme zu geben.

8.6.1 Schwarzfahrerdatei

Zur Frage der Zulässigkeit der Speicherung personenbezogener Daten strafunmündiger Kinder bei Schwarzfahrten im Verbundverkehr (11. TB S. 40) konnte mit der Deutschen Bundesbahn auch nach einem Gespräch auf Vorstandsebene keine Einigung erzielt werden. Die Deutsche Bundesbahn ist nach wie vor der Auffassung, daß die Erkennung von strafunmündigen Mehrfachtätern und die dadurch mögliche Einwirkung auf die Erziehungsberechtigten diese Speicherung rechtfertigen.

Ich stehe demgegenüber auf dem Standpunkt, daß die Deutsche Bundesbahn nach Zahlung des erhöhten Beförderungsentgelts kein berechtigtes Interesse mehr an der Speicherung der Daten strafunmündiger Kinder hat. Ein berechtigtes Interesse für die Speicherung dieser Daten kann nur geltend gemacht werden, solange ein zivilrechtlicher Anspruch auf Zahlung des erhöhten Beförderungsentgeltes besteht. Eine längere Speicherung kann für diesen Personenkreis weder mit einem — nicht vorhandenen — Strafanspruch nach § 265a StGB noch mit einem vermeintlichen Recht der Deutschen Bundesbahn zur Unterrichtung der Erziehungsberechtigten bei Wiederholungstätern begründet werden. Diese Auffassung vertreten ausnahmslos auch die Landesbeauftragten für den Datenschutz, die ich wegen ihrer Zuständigkeit für die übrigen an Verkehrsverbünden beteiligten kommu-

nalen Verkehrsbetriebe um Stellungnahme hierzu gebeten hatte.

Der Deutschen Bundesbahn steht es frei, im Rahmen der Erhebung des erhöhten Beförderungsentgelts die Erziehungsberechtigten auf die jeweiligen Schwarzfahrten hinzuweisen und zu bitten, auf die Kinder belehrend einzuwirken. Dies gilt auch für Wiederholungstaten; insoweit sind Hinweise der Deutschen Bundesbahn auf die begangenen Schwarzfahrten im Rahmen des jeweiligen Verfahrens zur Erhebung des erhöhten Beförderungsentgelts gerechtfertigt. Nach Zahlung dieses Entgelts kann es hingegen nur noch Aufgabe der Erziehungsberechtigten und nicht der Deutschen Bundesbahn sein, die Kinder von der Rechtswidrigkeit ihres Tuns zu überzeugen.

Auch sonstige Gründe für die Notwendigkeit einer Datenspeicherung nach Zahlung des Entgelts sind nicht erkennbar. Insbesondere läßt § 12 Abs. 2 Satz 1 der Eisenbahnverkehrsordnung keinen Ermessensspielraum für die Festsetzung eines höheren Entgelts im Wiederholungsfalle zu. Die Datenspeicherung ist deshalb zur Wahrung berechtigter Interessen nicht erforderlich und beeinträchtigt die schutzwürdigen Belange der Betroffenen.

Die Deutsche Bundesbahn ist auch nicht durch die Mitgliedschaft in einem Verkehrsverbund daran gehindert, die Daten strafunmündiger Kinder nach Zahlung des erhöhten Beförderungsentgelts zu löschen, denn Rechtsbeziehungen sind nur zwischen den einzelnen Gesellschaften des Verkehrsverbundes und den jeweiligen Fahrgästen entstanden.

Die Speicherung der Daten strafunmündiger Kinder durch die Deutsche Bundesbahn nach Zahlung des erhöhten Beförderungsentgelts ist nicht mit § 3 i. V. m. § 23 BDSG zu vereinbaren. Diese durch einige Bundesbahndirektionen praktizierte Datenverarbeitung habe ich daher gegenüber dem Vorstand der Deutschen Bundesbahn gemäß § 20 Abs. 1 BDSG beanstandet. Die Deutsche Bundesbahn hat ihre gegenteilige Position unverändert aufrecht erhalten.

8.6.2 Schülerbeförderung

Die Deutsche Bundesbahn rechnet Kosten der Beförderung von Schülern mit den nach den jeweiligen Landesgesetzen bestimmten Kostenträgern ab.

Ein Landesbeauftragter für den Datenschutz hat an mich die Frage herangetragen, ob bei der Rückerstattung wegen einer mit „Ausgehunfähigkeit" verbundenen Krankheit eines Schülers die Deutsche Bundesbahn die namentliche Krankmeldung des Schülers und die ärztlichen Atteste für Abrechnungszwecke benötigt. Seiner Auffassung nach braucht die Deutsche Bundesbahn für Abrechnungszwecke lediglich die Zahl der erkrankten Schüler und der Krankheitstage. Ich habe der Deutschen Bundesbahn daraufhin Lösungsvorschläge zur Reduzierung des Umfanges der Datenübermittlung unterbreitet.

Die Deutsche Bundesbahn ist nunmehr bereit, auf die generelle Vorlage der ärztlichen Bescheinigung bei einer mit „Ausgehunfähigkeit" verbundenen Krankheit von mehr als vierzehn Tagen grundsätzlich zu verzichten, wenn der Kostenträger in den Kostenerstattungsanträgen bescheinigt, daß ihm die ärztlichen Atteste oder Krankenhausbescheinigungen vorliegen. Die Deutsche Bundesbahn läßt sich jedoch das Recht einräumen, die Angaben durch Einsicht in die Bescheinigungen zu kontrollieren. Nach Mitteilung der Deutschen Bundesbahn ist allerdings die Übermittlung des Schülernamens zur ordnungsgemäßen Abwicklung der Kostenerstattung erforderlich.

Diese neuen Regelungen begrüße ich, weil damit Übermittlungen personenbezogener Daten nur in dem Umfang verlangt werden, die für die Aufgabenerfüllung tatsächlich erforderlich sind.

9 Statistik

9.1 Novellierung der Verknüpfungsregelung des § 13 Abs. 1 Nr. 3b) BStatG

Ich habe bereits an anderer Stelle (vgl. 9. TB S. 44 und 11. TB S. 41 und 42) über die Möglichkeit der Zusammenführung der aufgrund von einzelnen Wirtschafts- und Umweltstatistikgesetzen gewonnenen statistischen Erhebungen unter Inanspruchnahme der sog. Adreßdateien nach § 13 des Bundesstatistikgesetzes (BStatG) berichtet und auf die Gefahr hingewiesen, daß bei so gewonnenen Angaben von Einzelhandelskaufleuten (als natürlichen Personen) aussagekräftige Teilabbilder entstehen können, die das Recht auf informationelle Selbstbestimmung berühren.

Über die Auslegung der in § 13 Abs. 1 BStatG eingangs enthaltenen Voraussetzung „soweit ... erforderlich" ist es schon unmittelbar nach Verabschiedung des Gesetzes zu Meinungsverschiedenheiten innerhalb der Bundesregierung und zwischen dem BMI und mir gekommen. Ich habe zunächst die Auffassung vertreten, daß über die Erforderlichkeit von Verknüpfungen nur — wie bisher auch (vgl. z. B. §§ 3, 7 Agrarberichterstattungsgesetz 1980) — der Einzelgesetzgeber nach Maßgabe des Fachrechts befinden kann, Zusammenführungen im Sinne der Vorschrift also nicht von der Verwaltung für jede unter § 13 fallende Statistik angeordnet werden können. Deshalb habe ich darauf gedrungen, bei der Novellierung von Statistikgesetzen bereichsspezifische Verknüpfungsregelungen zu schaffen. So habe ich erreicht, daß in dem während des Berichtszeitraums verabschiedeten Agrarstatistikgesetz, über das ich bereits berichtet habe (11. TB S. 41 f.), die zunächst vorgesehene Regelung über die Möglichkeit einer Verknüpfung von Daten aus Landwirtschaftsstatistiken mit Daten aus allen anderen Wirtschaftsstatistiken gestrichen wurde. Nunmehr ist im neuen § 53 Agrarstatistikgesetz eine Regelung enthalten, wonach für Verknüpfungen lediglich die Erhebungsmerkmale aus einigen dort im einzelnen namentlich aufgeführten Statistiken verwendet werden dürfen (s. nachfolgend 9.2).

Wie ich bereits an anderer Stelle berichtet habe (11. TB S. 42 f.), war im Entwurf des Bundesministers für Arbeit und Sozialordnung für eine Änderung des Lohnstatistikgesetzes in ähnlicher Weise zunächst eine Regelung vorgesehen, die die Verknüpfung personenbezogener Angaben über die Auskunftspflichti-

gen mit Angaben von allen nachfolgenden Erhebungen nach dem Lohnstatistikgesetz sowie mit allen sonstigen Wirtschaftsstatistiken vorsah. Meine zunächst angestrebte Präzisierung des Ausschlusses von statistischen Zuordnungen, Zusammenführungen und Auswertungen im Sinne von § 13 BStatG im Lohnstatistikgesetz habe ich nicht weiter verfolgt, nachdem die Bundesregierung gegenüber dem federführenden Bundestagsausschuß für Arbeit und Sozialordnung sowie in der Begründung zum Lohnstatistikgesetz klargestellt hat, daß solche Verarbeitungen nicht beabsichtigt seien (s. 9.8).

Bei der Novellierung weiterer Statistikgesetze aus dem Bereich Wirtschaft und Umwelt stellt sich die gleiche Problematik. Es sollte aber nicht in jedem neuen Statistikgesetz um bereichsspezifische Regelungen gerungen werden, die die Anwendung (oder Nichtanwendung) des § 13 BStatG näher regeln. Ich habe deshalb der Entscheidung der Bundesregierung zugestimmt, aus Anlaß der Novellierung des Rohstoffstatistikgesetzes § 13 BStatG in der Weise zu ergänzen, daß für die in § 13 Abs. 1 Nr. 3 Buchstabe b) BStatG genannten statistischen Zuordnungen, Zusammenführungen und Auswertungen zusätzliche datenschutzrechtliche Sicherungen vorgesehen und zugleich die Vergabe einer Kenn-Nummer für jede Erhebungseinheit (auch zur Führung der Adreßdateien) ausdrücklich geregelt werden.

Mit dem Bundesminister des Innern, dem Bundesminister der Justiz und dem Statistischen Bundesamt habe ich dazu intensive Gespräche geführt. Diese haben zu der Übereinstimmung geführt, das Bundesstatistikgesetz durch einen § 13a zu ergänzen. Nach der vorgesehenen Regelung dürfen Datensätze aus Wirtschafts- und Umweltstatistiken zusammengeführt werden, soweit es zur Gewinnung von Informationen ohne zusätzliche statistische Erhebungen erforderlich ist. Die Zusammenführungen dürfen jedoch nur mittels einer Nummer erfolgen, die keinen Rückgriff auf die im künftigen § 13 Abs. 2 BStatG zusätzlich eingeführte Kenn-Nummer erlaubt, weil über diese eine Identifizierung des einzelnen Wirtschaftsbetriebes möglich wäre. Dies bedeutet in der Praxis, daß es unmöglich ist, das durch Zusammenführungen gewonnene umfassende statistische Datenbild einem einzelnen Auskunftspflichtigen zuzuordnen. Das so gefundene Ergebnis ist ein tatsächlich anonymes Zahlenwerk, dessen Erstellung mangels Kenntnis von Einzelpersonen oder -betrieben keinen Eingriff in das informationelle Selbstbestimmungsrecht Betroffener bedeutet. Unter dieser Voraussetzung war es mir möglich, meine Bedenken gegen die Zulassung von Verknüpfungen unterschiedlicher Statistiken zurückzustellen.

Leider konnte die beabsichtigte Änderung des § 13 BStatG bisher weder mit der Neufassung des Rohstoffstatistikgesetzes noch mit der Novellierung des Handwerkstatistikgesetzes verbunden werden. Die Bundesregierung beabsichtigt jedoch, die gebotene Neufassung der vorstehend beschriebenen Verknüpfungsregelung in eines der nächsten zur Beratung im Bundestag anstehenden Statistikgesetze aufzunehmen.

9.2 Agrarstatistikgesetz

Über das Agrarstatistikgesetz habe ich bereits in meinem Elften Tätigkeitsbericht (S. 41f.) berichtet. Im Laufe des Gesetzgebungsverfahrens konnte über die seinerzeit noch kontroversen Punkte Einvernehmen erzielt werden. Das neue Gesetz entspricht damit im wesentlichen den datenschutzrechtlichen Anforderungen. Insbesondere befriedigt die gefundene Regelung über die Verknüpfung verschiedener Agrarstatistiken (vgl. insoweit 9.1).

Ein wesentlicher Punkt war für mich, daß die den Betriebsinhaber, seinen Ehegatten sowie die auf dem Betrieb lebenden und dort mithelfenden Verwandten und Verschwägerten betreffenden Fragen von diesen Personen selbst auf jeweils einem eigenen Erhebungsbogen beantwortet werden können. Die Frage nach der außerbetrieblichen Tätigkeit und den sonstigen außerbetrieblichen Einkommensverhältnissen bei der Erhebung der sozialökonomischen Verhältnisse des Betriebsinhabers und seines Ehegatten wird nun so gestellt, daß die Erhebungsmerkmale nicht vom Betriebsinhaber jeweils für sich und seinen Ehegatten getrennt erfragt, sondern für das Betriebsinhaberehepaar zusammen erhoben werden. Dagegen habe ich mich mit meiner Anregung nicht durchsetzen können, Verwandte und Verschwägerte, die nur vorübergehend auf dem Betrieb leben und im Betrieb nicht mitarbeiten, bei den Fragen nach der sozialen Sicherung des Betriebsinhabers und seiner Familienangehörigen von der Auskunftspflicht zu entbinden.

Unter Hinweis auf die Zuständigkeit der Bundesländer für die Durchführung von Bundesstatistiken ist in das Gesetz — einem Vorschlag des Bundesrates folgend — eine Ermächtigung aufgenommen worden, wonach die Landesregierungen die erforderlichen Regelungen für die Bestimmung und Ausgestaltung der Erhebungsstellen durch Rechtsverordnung treffen können. Insoweit wurde meine Forderung, derartige Regelungen wegen ihrer Bedeutung für den Umfang des Grundrechtseingriffes im Gesetz selbst zu treffen, nicht aufgegriffen. Eine bundesgesetzliche Regelung hätte sicher der Rechtseinheitlichkeit und der Gesetzesökonomie gedient. Ob die Länder rechtzeitig und möglichst gleichlautend von der Verordnungsermächtigung Gebrauch machen werden, bleibt abzuwarten. In diesem Zusammenhang ist auch von Bedeutung, daß nur etwa die Hälfte der Bundesländer über Landesstatistikgesetze verfügt, die wenigstens eine allgemeine Bestimmung über die Abschottung der Erhebungsstellen von der übrigen Verwaltung enthalten. Die Kontrolle der Einrichtung und Ausstattung der Erhebungsstellen obliegt den Landesbeauftragten für den Datenschutz.

9.3 Ausländerstatistik

An anderer Stelle (s. oben 3.2) habe ich mich bereits zu dem vom Bundesminister des Innern vorgelegten Entwurf eines Gesetzes über das Ausländerzentralregister (AZRG) geäußert. Meiner in meinem Elften Tätigkeitsbericht (S. 45) geäußerten Kritik an der Rechtsgrundlage für die Ausländerstatistik hat der BMI

durch Neufassung der Regelung Rechnung getragen. Die einschlägige Vorschrift des § 17 AZRG kann als eigene Rechtsgrundlage für die Anordnung einer Bundesstatistik im Sinne des Bundesstatistikgesetzes angesehen werden. Sie enthält allerdings nicht ganz die nach § 9 Bundesstatistikgesetz erforderlichen Regelungen. So wurde beispielsweise meine Forderung, wenigstens eine Bestimmung über den Berichtszeitraum zu treffen, nicht aufgegriffen.

Es werden zudem so viele Einzelmerkmale erhoben, daß ich Bedenken habe, ob in allen Fällen eine hinreichende faktische Anonymisierung möglich ist. Eine solche ist insbesondere deshalb erforderlich, weil eine Unterrichtung der Betroffenen unterbleibt. Leider ist der BMI auf meinen Vorschlag, auf die Bezeichnung der Ausländerbehörde zu verzichten und insofern nur einen regionalen Bezug (etwa den zuständigen Regierungsbezirk oder eine Gruppe von Ausländerbehörden) anzugeben, nicht eingegangen. Ich habe aber erreicht, daß eine Deanonymisierung insoweit erschwert wird, als anstelle des Merkmals „Tag der Geburt" lediglich das Merkmal „Monat und Jahr der Geburt" erhoben wird. Durchgesetzt habe ich mich auch mit meiner Forderung, die Regelung über Planungsdaten von der über statistische Daten zu trennen und dafür eine eigene Vorschrift zu schaffen.

Insgesamt handelt es sich bei dem gefundenen Kompromiß um eine datenschutzrechtlich noch akzeptable Lösung.

9.4 Mikrozensusgesetz

Die Geltungsdauer des 1985 vom Bundestag beschlossenen Gesetzes zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz) endet im Jahr 1990. Da der Mikrozensus für eine Vielzahl verschiedener Zwecke Daten bereitstellt, nimmt er im System der amtlichen Statistik eine zentrale Stellung ein, so daß er weiterhin erhoben werden soll. Bereits in meinem Ersten Tätigkeitsbericht (S. 18f.) habe ich mich mit den Fragen nach der Zulässigkeit bestimmter Erhebungsmerkmale und der Auskunftspflicht beim Mikrozensus beschäftigt. An der Aktualität dieser damals aufgeworfenen Fragen hat sich bis heute nichts geändert.

Im Juni 1989 hat der Wissenschaftliche Beirat für Mikrozensus und Volkszählung, über dessen Aufgaben ich bereits (s. 8. TB S. 27 und 9. TB S. 45) berichtet habe, seinen Bericht „Mikrozensus im Wandel — Untersuchungen zur inhaltlichen und methodischen Gestaltung" vorgelegt. Er kam zu dem Ergebnis, daß bei freiwilligen Erhebungen in keinem Fall mit einer erforderlichen, nahe an 100% reichenden Beteiligung zu rechnen sei. Freiwillige Auskunftserteilung führe keineswegs zu einer besseren Qualität der Ergebnisse, sondern werde vielmehr dazu genutzt, an der Befragung nicht teilzunehmen. Unter Einbeziehung der Erfahrungen im Ausland, der empirischen Sozialforschung und der Ergebnisse von Testerhebungen des Mikrozensus 1985 bis 1987 stehe fest, daß zwar für eine Reihe von Themenbereichen unter bestimmten Voraussetzungen die Auskunftserteilung auf freiwilliger Basis möglich sei. Für das Kernprogramm des Mikrozensus bleibe die Auskunftspflicht jedoch weiterhin erforderlich.

Unter Zugrundelegung dieses Berichts hat das Statistische Bundesamt einen Gesetzentwurf für ein neues Mikrozensusgesetz erarbeitet. Da der Entwurf jedoch eine erhebliche Ausweitung des Fragenkatalogs — allerdings mit einer Ausdehnung von freiwillig zu beantwortenden Erhebungsmerkmalen — beinhaltete, ohne daß anderweitig eine fühlbare Reduzierung der Erhebungsmerkmale, für die Auskunftspflicht besteht, vorgenommen wurde, bestanden dagegen erhebliche Bedenken. Dies führte dazu, daß dieser Entwurf erfreulicherweise nicht weiterverfolgt wurde.

Unterstützt habe ich dagegen den Alternativentwurf des Bundesministers des Innern, der im wesentlichen die Verlängerung des jetzt geltenden Mikrozensusgesetzes vorsieht. Dieser Entwurf hält unter Berücksichtigung der Ergebnisse der eingangs genannten Testerhebungen und der grundsätzlichen Bedenken des Wissenschaftlichen Beirates gegen einen Verzicht auf die Auskunftspflicht im Kernprogramm des Mikrozensus an der Auskunftspflicht im wesentlichen fest. Er sieht aber auch vor, daß für eine Reihe von Erhebungsmerkmalen, für die bisher Auskunftspflicht bestand, nunmehr eine Befragung auf freiwilliger Basis erfolgen soll. Diese Entwicklung halte ich für richtig, wenn ich auch weiterhin noch gewisse Bedenken wegen des Umfanges der Erhebungsmerkmale habe. Daneben sieht der Entwurf Testerhebungen in den Jahren 1991 und 1992 zur Prüfung der Frage vor, ob in künftigen Mikrozensuserhebungen anstelle einer jährlichen Erhebung vierteljährliche Erhebungen durchgeführt werden können. Da der Auswahlsatz jährlich eins vom Hundert nicht übersteigen darf und in jedem Erhebungsbezirk jährlich nur eine Erhebung stattfinden soll, ist sichergestellt, daß damit auf die Bürger keine zusätzliche Belastung zukommt.

9.5 Gebäude- und Wohnungsstichprobe

Mit dem von der Bundesregierung beschlossenen Entwurf eines Gesetzes über die Durchführung einer Repräsentativstatistik auf dem Gebiet des Wohnungswesens (Gebäude- und Wohnungsstichprobengesetz) soll ein wesentlicher Teil aus der Regelung über den Mikrozensus ausgegliedert und in einem eigenen Gesetz behandelt werden. Der Bundesminister für Raumordnung, Bauwesen und Städtebau hat mich bei der Vorbereitung des Gesetzentwurfs beteiligt. Dabei konnte ich datenschutzrechtliche Verbesserungen erreichen. So wurde z. B. auf meine Anregung hin in den Gesetzesentwurf eine Regelung aufgenommen, wonach der Betroffene frei darüber entscheiden kann, ob er einen Erhebungsbogen für sich allein oder gemeinsam mit anderen Haushaltsmitgliedern beantworten will.

Meinen Bedenken gegen die Bestimmung des Entwurfs, die die Übermittlung von statistischen Ergebnissen an die obersten Bundes- und Landesbehörden regelt, wurde leider nicht Rechnung getragen. Es wurde mir aber versichert, die Möglichkeit, aus den übermittelten Daten Einzelpersonen zu reidentfizie-

ren, sei nahezu ausgeschlossen, weil den Stellen, die mit den Tabellen arbeiten, die Lage der in die Stichprobe gekommenen Auswahlbezirke unbekannt sei.

Bedenken habe ich auch gegen einzelne Erhebungsmerkmale vorgebracht. So habe ich deutlich gemacht, daß die Begriffe „soziale Stellung" und „Familienzusammenhang" einer näheren Konkretisierung im Gesetz bedürfen. Auch habe ich in Zweifel gezogen, ob es tatsächlich notwendig ist, den Geburtsmonat zu erfragen. Der BMBau hat mir zugesagt, meine Bedenken zu überprüfen. Auf meine vom BMJ unterstützte dringende Bitte hin, die Notwendigkeit des Erhebungsmerkmales „Form des Zusammenlebens und -wohnens" zu überprüfen, hat der Bundesminister nachdrücklich erklärt, daß gerade die Erhebung dieses Merkmals angesichts der zunehmenden Zahl eheähnlicher Gemeinschaften unverzichtbar sei; es stelle sich zunehmend als Mangel heraus, über diesen bereits mehrere Millionen Menschen umfassenden Personenkreis statistisch nichts zu wissen. Der Bundesminister beabsichtigt jetzt vorzuschlagen, daß die Frage nach dem Zusammenleben als Frage nach der „Zugehörigkeit zu einer Wohngemeinschaft" gestellt wird. Ob ich meine grundsätzlichen Bedenken gegenüber einer derartigen, stark in die persönliche Sphäre der Bürger eingreifenden Frage hintanstellen kann, kann ich erst beurteilen, wenn mir die geänderte Fassung des Erhebungskatalogs vorliegt. Hervorzuheben ist, daß auf eine gemeinsame Anregung mit dem BMJ hin sich der BMBau bereiterklärt hat, beim Erhebungsmerkmal „Höhe des monatlichen Nettoeinkommens nach Einkommensklassen" eine konkrete Staffelung in das Gesetz aufzunehmen.

9.6 Hochschulstatistikgesetz

Der Novellierungsentwurf des Gesetzes über die Statistik für das Hochschulwesen (Hochschulstatistikgesetz) trägt den Belangen des Datenschutzes im wesentlichen Rechnung.

Besonders bedeutsam ist die Tatsache, daß der Bundesminister für Bildung und Wissenschaft in dem Gesetzentwurf auf die von den Bundesländern gewünschte Studienverlaufsstatistik verzichtet hat. Gegen die vorgesehene Ausweitung der Erhebungsmerkmale und die Erschließung von neuen verlaufsanalytischen Auswertungsmöglichkeiten habe ich nichts einzuwenden, solange eine Identifizierung eines einzelnen Studenten nicht möglich ist. Auf Wunsch des Bundesrates soll in den Gesetzentwurf eine Befragung von Abiturienten aufgenommen werden, mit der die Studienwünsche der Schüler zu Planungszwecken ermittelt werden sollen. Da diese Befragung auf freiwilliger Basis erfolgen soll, bestehen dagegen aus datenschutzrechtlicher Sicht keine Bedenken.

Bedenken habe ich jedoch gegen den Vorschlag des Bundesrates geäußert, die Matrikel-Nummer als Hilfsmerkmal zu erheben. Die Erhebung der Matrikel-Nummer bietet, wenn sie auch das Geburtsdatum enthält, in einigen Bundesländer die Möglichkeit eines Abgleichs der Statistikdaten mit den Angaben des Vorsemesters und der Bereinigung der Fallzählung in den Hochschulverwaltungen. Dies wäre eine Verwendung für statistikfremde Aufgaben, die dem Grundsatz der strikten Trennung von Statistik und Verwaltungsvollzug widerspricht. Deshalb darf die Matrikel-Nummer allenfalls ausschließlich für Rückfragen beim Auskunftspflichtigen erhoben werden. Bedauerlicherweise habe ich mich mit meiner Auffassung nicht durchsetzen können. Die Bundesregierung hat vielmehr dem Vorschlag des Bundesrates zugestimmt. Sie hat allerdings in ihrer Gegenäußerung darauf hingewiesen, daß die Matrikel-Nummer gelöscht werden muß, sobald die Überprüfung der Erhebungs- und Hilfsmerkmale auf ihre Schlüssigkeit und Vollständigkeit abgeschlossen ist, und daß ihre gesonderte Aufbewahrung nach § 12 Abs. 2 BStatG sowie ihre Verwendung für einen Vergleich der Erhebungsmerkmale mit denjenigen aus der nachfolgenden Erhebung unzulässig sind. Ich hätte es begrüßt, wenn diese Auffassung nicht nur als Auslegungshinweis in die Gegenäußerung der Bundesregierung, sondern in den Gesetzestext aufgenommen worden wäre.

Nicht unproblematisch ist auch die vom Bundesrat vorgeschlagene und von der Bundesregierung in ihrer Gegenäußerung gebilligte Regelung, wonach Ergebnisse der Hochschulstatistik auf einzelne Hochschulen und einzelne Hochschulstandorte bezogen veröffentlicht werden dürfen. Gerade bei Studienfächern mit geringer Studentenzahl an kleineren Hochschulen können den statistischen Ergebnissen so kleine Mengen zugrunde liegen, daß mit geringem Zusatzwissen auf einen Studenten zurückgeschlossen werden kann.

9.7 Strafverfolgungsstatistikgesetz

Der Bundesminister der Justiz hat mir einen Arbeitsentwurf eines Strafverfolgungsstatistikgesetzes zugeleitet, dessen datenschutzrechtliche Hauptproblematik in der Mitwirkung des Bundeszentralregisters an der künftigen Strafverfolgungsstatistik liegt.

Dem Bundeszentralregister sollen von den Geschäftsstellen der Gerichte und Staatsanwaltschaften statistische Daten sowie Daten, die nur zu Verwaltungszwecken erhoben wurden, gemeinsam — wenn auch möglicherweise auf einem jeweils eigenen Datenträger — übermittelt werden. Das BZR soll sodann nach Erfassung der Daten für Registerzwecke den Statistischen Landesämtern monatlich die statistischen Daten übermitteln. Wenn auch die Aufbereitung der Statistik im BZR in einer abgeschotteten Organisationseinheit erfolgen soll, habe ich gegen das Verfahren im Hinblick auf den verfassungsrechtlich gebotenen Grundsatz der Trennung von Statistik und Verwaltungsvollzug datenschutzrechtliche Bedenken. Diese ergeben sich insbesondere daraus, daß nach dem bisherigen Konzept noch unklar ist, wann die statistischen Daten von den Daten, die auch zu Verwaltungszwecken erhoben wurden, getrennt werden.

In meiner Stellungnahme habe ich mich auch gegen die Erhebung der Geschäftsnummer des Gerichts oder der Staatsanwaltschaft als Hilfsmerkmal gewandt, weil mit ihrer Hilfe der Zugang zu den Gerichtsakten und damit zur Person des Betroffenen ermöglicht wird. Ich habe dem BMJ deshalb vorgeschlagen, daß für etwaige Rückfragen anstelle der Geschäftsnummer eine nicht sprechende Kenn-Nummer als Identifikator verwendet wird.

Der Bundesminister wurde von mir ferner gebeten zu erwägen, ob die Schaffung des Strafverfolgungsstatistikgesetzes nicht dazu genutzt werden sollte, das Bundeszentralregister gänzlich von statistischen Aufgaben zu befreien. Der beabsichtigte Verwaltungsvereinfachungseffekt könnte m. E. auch dadurch erzielt werden, daß die Meldungen der auskunftsgebenden Stellen an das Bundeszentralregister und das Statistische Landesamt auf durchschreibenden Erhebungsbogen erteilt und jeweils gesondert an die Empfänger versandt werden. Der vom Bundesminister angeführte Einsparungseffekt durch das zentrale Einlesen der Erhebungsbogen beim Bundeszentralregister dürfte mit der zunehmenden Ausstattung der Geschäftsstellen von Gerichten und Staatsanwaltschaften mit Datenverarbeitungsanlagen erheblich an Bedeutung verlieren. Wegen der Vielzahl und Schwere der derzeit noch ungeklärten datenschutzrechtlichen Probleme habe ich den Bundesminister gebeten, von einem beabsichtigten Probelauf in drei Landgerichtsbezirken abzusehen oder bei dem Probelauf keine Originaldaten zu verwenden.

9.8 Lohnstatistikgesetz

Wie ich bereits in meinem Elften Tätigkeitsbericht (S. 42f.) berichtet habe, habe ich mich insbesondere gegen die namentliche Übermittlung sensibler Arbeitnehmerdaten wie Bruttoverdienst und Qualifikation im Neuentwurf des Lohnstatistikgesetzes gewandt. Diese Regelung ist zwar im inzwischen verabschiedeten Gesetz nicht gänzlich gestrichen worden; ich habe jedoch erreichen können, daß der Name des in die Erhebung einzubeziehenden Arbeitnehmers nur dann als Hilfsmerkmal verwendet werden darf, wenn der auskunftspflichtige Arbeitgeber keine — den Namen des Arbeitnehmers ersetzende — betriebliche Kennziffer zur Statistik gemeldet hat. Für diesen Fall ist in das Gesetz eine Verpflichtung des Arbeitgebers aufgenommen worden, den betroffenen Arbeitnehmer über die Meldung seiner personenbezogenen Daten zur Statistik zu unterrichten. Diese Regelungen enthalten eine deutliche Verstärkung des Rechts auf informationelle Selbstbestimmung und entsprechen den Anforderungen einer aussagefähigen Statistik.

Im übrigen hatte ich mich im Elften Tätigkeitsbericht gegen die Streichung der präzisen Regelung über die zeitweilige Aufbewahrung von Namen und Anschriften von auskunftspflichtigen Arbeitgebern sowie Namen und Kennziffern der betroffenen Arbeiter gewandt. Die Aufhebung dieser Regelung hätte es möglich gemacht, die viel weitergehende Vorschrift des § 13 BStatG anzuweden. Ich habe deshalb akzeptiert, daß die bisherige Aufbewahrungsvorschrift in der Neufassung des Lohnstatistikgesetzes erhalten geblieben ist.

9.9 Ausbildungsförderungsstatistik

Sowohl im Zehnten (S. 62f.) als auch im Elften Tätigkeitsbericht (S. 44) habe ich über die datenschutzrechtlich bedenkliche Datenerhebung durch die Ämter für Ausbildungsförderung nach § 55 Abs. 3 des Bundesausbildungsförderungsgesetzes (BAföG) berichtet. Auf meine Intervention hin hat der Bundestagsausschuß für Bildung und Wissenschaft davon abgesehen, eine von der Bundesregierung vorgeschlagene Regelung der Ausbildungsförderungsstatistik zu verabschieden, die weder unter datenschutzrechtlichen noch unter statistisch-fachlichen Gesichtspunkten befriedigen konnte.

Im Entwurf zum Zwölften Gesetz zur Änderung des BAföG hat der Bundesminister für Bildung und Wissenschaft nunmehr meinen Bedenken Rechnung getragen. Auf meine Zweifel, ob die in § 55 BAföG enthaltenen Erhebungsmerkmale von den Ämtern für Ausbildungsförderung zur Durchführung des Gesetzes und nicht lediglich zu statistischen Zwecken benötigt werden, hat mir der Bundesminister ausdrücklich und plausibel versichert, daß jedes im Entwurf genannte Erhebungsmerkmal für Zwecke der Durchführung des Gesetzes zwingend erforderlich ist. Durch die Neufassung des § 55 Abs. 3 und 4 BAföG werden, wie von mir vorgeschlagen, die Regelungen über die Hilfsmerkmale und die Auskunftspflicht den Anforderungen des Bundesstatistikgesetzes angepaßt. Bei der nunmehr erforderlichen Umstellung des von den Ämtern für Ausbildungsförderung benutzten Erhebungsbogens (Formblatt) werde ich den BMBW beraten.

10 Wissenschaft und Forschung

10.1 Forschungsklauseln in neueren Gesetzen

Im Berichtszeitraum sind mir weitere Gesetzentwürfe zugeleitet worden, die Regelungen über die Informationsübermittlung für wissenschaftliche Zwecke (Forschungsklauseln) enthielten.

Der vom Bundesminister der Justiz vorgelegte *Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts,* über den ich an anderer Stelle (s. 4.1) bereits berichtet habe, enthält eine entsprechende Ergänzung der Strafprozeßordnung. Danach können Hochschulen und andere Forschungseinrichtungen Akteneinsicht oder Auskunft aus Strafverfahrensakten erhalten, soweit dies für die Durchführung bestimmter wissenschaftlicher Forschungsarbeiten erforderlich ist und das öffentliche Interesse an der Forschungsarbeit das schutzwürdige Interesse der Betroffenen an dem Ausschluß der Akteneinsicht oder Aktenauskunft erheblich überwiegt.

Der Entwurf bringt gegenüber einer früheren Fassung den Vorrang von Berufs- und besonderen Amtsgeheimnissen sowie sonstiger Geheimhaltungsregelungen gegenüber Forschungsinteressen weniger deutlich zum Ausdruck. Er berücksichtigt auch nicht

meine Forderung, wenigstens grundsätzlich die Einwilligung des Betroffenen als Voraussetzung für die Nutzung seiner Daten zu Forschungszwecken festzulegen. Zusätzlich habe ich als weitere Voraussetzung für die Auskunftserteilung aus Strafakten vorgeschlagen, daß der Zweck der Forschung nicht auf andere Weise erreicht werden kann. Mein Vorschlag entspricht den Regelungen in § 33 Abs. 1 Satz 2 des Hessischen Datenschutzgesetzes und § 28 Abs. 2 des Datenschutzgesetzes von Nordrhein-Westfalen. Für den Fall der Überlassung von personenbezogenen Daten an nicht-öffentliche Stellen zu Forschungszwecken habe ich schließlich angeregt, dem Beispiel des § 33 Abs. 4 des Hessischen Datenschutzgesetzes zu folgen, wonach eine Übermittlung von Daten an eine solche Stelle nur erfolgen darf, wenn sich der private Empfänger der Kontrolle des Datenschutzbeauftragten unterwirft. Auch diese Empfehlungen sind bisher nicht in den Gesetzentwurf übernommen worden.

Die gleichen Hinweise und Bedenken habe ich auch gegen die im *Novellierungsentwurf des Bundeszentralregistergesetzes* enthaltene Forschungsklausel geltend gemacht, die erkennbar der entsprechenden Vorschrift im Strafverfahrensänderungsgesetz nachgebildet ist.

Bedenken habe ich auch gegen den Vorschlag des BMJ geäußert, *§ 78 des Zehnten Buches des Sozialgesetzbuches* (SGB X) durch einen Absatz 2 in der Weise zu ergänzen, daß in Strafakten oder in einer entsprechenden Datei befindliche Jugendgerichtshilfeberichte und andere unter das Sozialgeheimnis fallende personenbezogene Daten zum Zweck der wissenschaftlichen Forschung ohne Rücksicht auf die besonderen Offenbarungsregelungen des Sozialgesetzbuches unter den Voraussetzungen der in die Strafprozeßordnung einzufügenden Forschungsklausel übermittelt werden können. Ich verkenne nicht, daß die Anwendung einheitlicher Vorschriften die Praktikabilität der Bereitstellung von Daten aus Gerichtsakten für Forschungszwecke erhöht. Gleichwohl sollte nicht der Aufbewahrungsort (Gerichtsakten) von Daten, sondern ihre Sensibilität entscheidend sein. Ich habe den BMJ auf bereits bestehende bereichsspezifische Forschungsklauseln hingewiesen. So dürfen nach § 287 Abs. 2 des Fünften Buches des Sozialgesetzbuches (SGB V) Forschungsvorhaben nur mit anonymisierten und damit nicht personenbeziehbaren Daten durchgeführt werden. Es besteht für mich kein erkennbarer Grund, für andere unter das Sozialgeheimnis fallende Daten von dieser Regelung abzuweichen.

10.2 Forschungsvorhaben „Anonymisierung"

Im Elften Tätigkeitsbericht (S. 48) hatte ich über ein Forschungsvorhaben berichtet, das der Lehrstuhl für Methoden der empirischen Sozialforschung und angewandte Soziologie der Universität Mannheim zusammen mit dem Statistischen Bundesamt und unter Mitwirkung des Zentrums für Mikrodaten, einer Abteilung des Zentrums für Umfragen, Meinungen und Analysen (ZUMA), Mannheim, durchführt.

Das ursprünglich ins Auge gefaßte Ziel, Ergebnisse bereits im September 1989 vorzustellen, konnte nicht verwirklicht werden. Die Beschaffung originaler Daten sowie weiterer sozialwissenschaftlicher Erhebungen zur Überprüfung von Anonymisierungsmaßnahmen erforderte eine intensive Abstimmung zwischen den beteiligten Stellen. Die ZUMA wird nunmehr vom Landesamt für Datenverarbeitung und Statistik Nordrhein-Westfalen die für die Durchführung des Projektes erforderlichen Daten erhalten. Die Verzögerung beruht auch darauf, daß für die Überprüfung eine vorab nicht eingeplante Quelle von Zusatzwissen zusätzlich berücksichtigt werden mußte. Entgegen der ursprünglichen Absicht, nur das in meinem Elften Tätigkeitsbericht erwähnte, von der Gesellschaft für Mathematik und Datenverarbeitung (GMD) entwickelte Verfahren anzuwenden, soll nunmehr wegen der Probleme bei der praktischen Umsetzung dieser komplexen Methode ein weiteres, relativ einfaches Verfahren in die empirischen Tests mit aufgenommen werden. Aus diesem Grund wurde die Laufzeit des Projektes um neun Monate verlängert, so daß die Ergebnisse nunmehr im Juni 1990 vorgestellt werden sollen.

10.3 Gentechnologie

Im Elften Tätigkeitsbericht habe ich berichtet, daß sich unter meiner Federführung eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit verschiedenen Themen beschäftigt, die im Bericht der Enquete-Kommission „Chancen und Risiken der Gentechnologie" (Bundestags-Drucksache 10/6775) als datenschutzrelevant ausgewiesen sind. Nach fachlicher Beratung hat die Arbeitsgruppe als Hilfe für die Datenschutzbeauftragten des Bundes und der Länder ein Diskussionspapier „Genomanalyse und informationelle Selbstbestimmung" erarbeitet, in dem außer einem allgemeinen Teil Überlegungen zur Verwendung der Genomanalyse im gerichtlichen Verfahren, bei Arbeitnehmern, im Versicherungswesen, bei der pränatalen Diagnostik und beim Neugeborenen-Screening enthalten sind. Am 26./27. Oktober 1989 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz die in Anlage 7 abgedruckte Entschließung „Genomanalyse und informationelle Selbstbestimmung" gefaßt.

Die Beschlußempfehlung und der Bericht des Ausschusses für Forschung und Technologie (Drucksache 11/5320) zum Bericht der Enquete-Kommission „Chancen und Risiken der Gentechnologie", der Änderungsantrag der Fraktion der SPD hierzu (Drucksache 11/5468) und die noch nicht abgeschlossenen Überlegungen der unter Federführung des Bundesministers der Justiz arbeitenden Bund-Länder-Arbeitsgruppe „Genomanalyse" machen deutlich, daß in diesem schwierigen Bereich sicherlich nicht in Kürze mit Ergebnissen in Form von Rechtsnormen zu rechnen ist, die alle auftretenden Fragen regeln. In der Öffentlichkeit wird aber gerade dieses als Mangel empfunden, da die Genomanalyse z. B. im gerichtlichen Verfahren schon angewandt wird. Es ist deshalb notwendig, möglichst rasch für diese Bereiche Rechtsnormen

zu schaffen, die die Praxis steuern, damit nicht umgekehrt der Gesetzgeber durch bereits geübte Verfahren und Praktiken vor vollendete Tatsachen gestellt wird und nur noch nachvollziehen kann, was Gerichte und Verwaltung bereits vorentschieden haben.

11 Sozialwesen — Allgemeines —

11.1 Sozialversicherungsausweisgesetz

Mit dem Gesetz vom 6. Oktober 1989 wurde durch Ergänzung des SGB IV die Einführung des Sozialversicherungsausweises ab 1991 in Verbindung mit flankierenden neuen Meldevorschriften, u. a. auch für geringfügig Beschäftigte, die bereits ab Anfang 1990 gelten, beschlossen. Meine im Elften Tätigkeitsbericht (S. 50/51) zum Ausdruck gebrachte Hoffnung, im Gesetzgebungsverfahren noch einige bereits vorgeschlagene datenschutzrechtlichen Verbesserungen zu erreichen, hat sich im wesentlichen erfüllt.

Eignung und Erforderlichkeit des Sozialversicherungsausweises für den Gesetzeszweck der Aufdekkung von illegalen Beschäftigungsverhältnissen und von Leistungsmißbrauch erscheinen mir plausibel begründet, zumal seine Effizienz durch Meldepflichten und Kontrollen verstärkt wird.

Meine Anregungen wurden insbesondere in folgenden Punkten aufgegriffen:

— Von der Anwendung des Gesetzes wurden geringfügig Beschäftigte bis zum vollendeten 16. Lebensjahr, die eine allgemeinbildende Schule besuchen, ausgenommen; nicht akzeptiert wurde meine Anregung, auch Beschäftigte mit einer Minimalvergütung — etwa 100,— DM monatlich — auszunehmen.

— Aufgrund meiner Bedenken gegen die Anregung des Bundesrates, den Sozialversicherungsausweis generell mit einem Lichtbild auszustatten, wurde dies auf die Fälle derjenigen Beschäftigten beschränkt, die den Sozialversicherungsausweis mitzuführen haben. M. E. hätte es sogar ausgereicht, in diesen Fällen die Mitführung eines mit Lichtbild versehenen gültigen amtlichen Ausweises in Verbindung mit dem Sozialversicherungsausweis vorzusehen.

— Der Gesetzentwurf wurde in § 95 Abs. 3 durch ein klares grundsätzliches Verbot ergänzt, den Sozialversicherungsausweis zum automatisierten Abruf personenbezogener Daten zu verwenden. Dies dürfen ausnahmsweise lediglich die Bundesanstalt für Arbeit, die Krankenkassen als Einzugsstellen sowie die Träger der Rentenversicherung und das auch nur, soweit es für den Gesetzeszweck erforderlich ist.

  Außerdem ist der Kreis der Daten, die auf diesem Weg abgerufen werden können, auf Daten über Meldungen zur Sozialversicherung, Kontrollmeldungen nach § 102, Sofortmeldungen nach § 103, Meldungen für geringfügig Beschäftigte nach § 104, auf Daten zum Leistungsbezug bei der Bundesanstalt für Arbeit und über erteilte Arbeitserlaubnisse abschließend begrenzt worden.

— Der Sozialversicherungsausweis darf nur für die in § 95 Abs. 1 genannten Zwecke und die Erhebung der Versicherungsnummer verwendet werden. Ebenso präzise wurden die Behörden bestimmt, denen der mitzuführende Sozialversicherungsausweis vorzulegen ist.

— Die Meldungen für geringfügig Beschäftigte nach § 104 sind bei der Datenstelle des Verbandes der Rentenversicherungsträger (VDR) in einer besonderen Datei zu führen. Diese Regelung war im Vorfeld verschiedentlich angegriffen worden. Sie ist aber vor allem deswegen datenschutzrechtlich gerechtfertigt, weil durch diese zentrale Dateiführung zum einen der Gesetzeszweck am ehesten erreicht und zum anderen die strikte Abschottung von den Daten der Rentenversicherten ebenso gewährleistet wird, wie mehr Transparenz für die Betroffenen und die Kontrollinstanzen. Die Speicherungsdauer der Daten wird nach dem Erforderlichkeitsprinzip auf fünf Jahre nach Ablauf des Kalenderjahres, in dem die Abmeldung erfolgt ist, begrenzt (§ 105 Abs. 3).

— Soweit durch die Vorschrift des § 95 Abs. 3 auch die Vorentscheidung für eine Maschinenlesbarkeit des Sozialversicherungsausweises getroffen worden ist, habe ich hiergegen insbesondere deswegen keine datenschutzrechtlichen Bedenken, weil dieses Verfahren — abgesehen von seinen Rationalisierungseffekten — die Anzahl der für Kontrollzwecke zu erhebenden und zu speichernden personenbezogenen Daten der Beschäftigten auf die Verdachtsfälle beschränkt.

11.2 See-Berufsgenossenschaft — Seekasse

See-Berufsgenossenschaft und Seekasse mit der ihr angegliederten Seekrankenkasse sind zwei bundesunmittelbare Körperschaften des öffentlichen Rechts, bilden aber eine Verwaltungsgemeinschaft unter gemeinsamer Geschäftsführung. Getrennt nach den einzelnen Zweigen der Seemännischen Sozialversicherung (Kranken-, Renten- und Unfallversicherung) werden die Sach- und Barleistungen jeweils in eigenständigen Abteilungen erbracht. Die für alle Zweige gemeinsam anfallenden Aufgaben werden in Gemeinschaftsabteilungen erledigt, so z. B. Mitgliederverwaltung, Beitragseinzug, Gesundheitsabteilung/ Medizinischer Dienst. Hierzu bedienen sich die Träger der Seemännischen Sozialversicherung in Teilbereichen auch eines bei der See-Berufsgenossenschaft angesiedelten eigenen Rechenzentrums und für den Bereich der Versicherungskontenführung der Rentenversicherung der Arbeiter des gemeinsam betriebenen Rechenzentrums bei der LVA Hamburg. Durch diese besondere Organisationsform entstehen datenschutzrechtlichen Probleme (s. 11.5).

Die Organisation des Datenschutzes bei den Trägern der Seemännischen Sozialversicherung entspricht den gesetzlichen Anforderungen. Als Ergebnis einer

Kontrolle habe ich darüber hinaus im wesentlichen folgende Anregungen gegeben:

— Die Dienstanweisung zum Datenschutz und der jährlich vom internen Datenschutzbeauftragten erstellte Bericht, der auch Hinweise zur Lösung der aufgetretenen datenschutzrechtlichen Probleme enthalten soll, sollte allen Mitarbeitern zugänglich gemacht werden;

— die Belange des Datenschutzes sollten regelmäßiger Inhalt der Führungskräftebesprechungen und der Aus- und Fortbildung aller Mitarbeiter sein;

— die Datenübersicht nach § 15 BDSG sollte durch eine Aufstellung der aus den Dateien erstellten Anwendungen ergänzt werden;

— der Datenschutzbeauftragte sollte alle Protokollierungen auswerten, die der Kontrolle der Sicherheit der Datenverarbeitungsverfahren dienen;

— die datenschutzrechtlichen Hinweise in Vordrucken sollten die Rechtsgrundlagen der Datenerhebung (u. a. § 9 Abs. 2 BDSG, §§ 60ff. SGB X, 76 Abs. 2 SGB X), die Rechte und Pflichten und deren Bedeutung für die Betroffenen verständlich wiedergeben;

— Arztgutachten sowie Befundberichte sollten, soweit diese in den Aktenvorgängen enthalten sind, in verschlossenem Umschlag, dessen Öffnung jeweils unter Angabe von Zeitpunkt, Zweck/Anlaß und Name des (der) Sachbearbeiters(in) zu protokollieren ist, verwahrt werden.

Ich habe meine Kontrolle auch zum Anlaß genommen, die bisherige Umsetzung des Gesundheitsreformgesetzes zu prüfen (s. auch 13.1). Dabei konnte ich keine nennenswerten Defizite feststellen.

See-Berufsgenossenschaft und Seekasse haben meine Empfehlungen aufgegriffen, weitgehend umgesetzt und im übrigen eine baldige Klärung zugesagt.

11.3 Versorgungsanstalt der Deutschen Bundespost

Die Versorgungsanstalt der Deutschen Bundespost (VAP) ist eine Sozialeinrichtung der Deutschen Bundespost, die ihren Versicherten und deren Hinterbliebenen u. a. eine zusätzliche Alters- und Hinterbliebenenversorgung gewährt. Sie ist als rechtsfähige Anstalt des öffentlichen Rechts fachlich nicht weisungsgebunden, unterliegt jedoch der Dienstaufsicht des Sozialamts der Deutschen Bundespost (SAP).

Im Rahmen einer Kontrolle habe ich insbesondere die Organisation des Posteingangsverfahrens der VAP geprüft. Die Post wurde von Mitarbeitern des SAP beim zuständigen Postamt abgeholt, in der der Fachaufsicht des SAP unterstehenden Posteingangsstelle geöffnet, in das entsprechende Fach der VAP einsortiert und anschließend in verschlossenen Behältern zur VAP transportiert. Nach meinen Feststellungen enthält die Eingangspost der VAP Schriftstücke mit besonders sensiblem Inhalt wie Scheidungsurteile, Mitteilungen über Versorgungsbezüge, ärztliche Gutachten, usw.

Ich habe diese Organisation des Posteingangsverfahrens als Verstoß gegen die Pflicht zur Wahrung des Sozialgeheimnisses gemäß § 35 SGB I sowie die Grundsätze zur Wahrung des Personaldatenschutzes und des Schutzes von Gesundheitsdaten beanstandet. Diese Organisation ermöglichte den mit der Öffnung der Postvorgänge betrauten Mitarbeitern des SAP die Kenntnisnahme vom Inhalt an die VAP gerichteter höchst sensibler Daten, ohne daß dies aus der fachlichen Aufgabenzuweisung des SAP heraus erforderlich ist und die Betroffenen davon erfahren.

Auf meine Empfehlung hin wurde die Bearbeitung der Eingangspost der VAP einschließlich des Posttransports vorläufig vom SAP zur VAP verlagert. Eine Besprechung der Problematik mit Vertretern des Bundesministers für Post und Telekommunikation, des SAP sowie des Bundesrechnungshofes ergab, daß die gemeinsame Posteingangsstelle für das SAP und die angegliederten Selbstverwaltungseinrichtungen künftig der VAP zugeordnet und der Fachaufsicht der Geschäftsführung der VAP unterstellt werden sollen. Hinsichtlich weiterer Einzelheiten einer datenschutzgerechteren Verfahrensweise bin ich weiterhin mit dem Bundesminister für Post und Telekommunikation im Gespräch.

11.4 Bundesknappschaftsälteste

Aufgrund einer Eingabe habe ich mich im Berichtsjahr mit der Aufgabenwahrnehmung der ehrenamtlich tätigen Knappschaftsältesten bei der Bundesknappschaft befaßt. Diesen kommt nach § 39 Abs. 3 SGB IV insbesondere die Aufgabe zu, eine ortsnahe Verbindung des Versicherungsträgers mit den Versicherten und den Leistungsberechtigten herzustellen, diese zu beraten und zu betreuen.

In dem der Eingabe zugrunde liegenden Fall war es im Zusammenhang mit der Zustellung eines Schreibens durch einen Knappschaftsältesten zu einer Verletzung des Sozialgeheimnisses nach § 35 SGB I gekommen.

Ich habe diesen Fall zum Anlaß genommen, die Bundesknappschaft darum zu bitten, ihr Zustellungsverfahren neu zu regeln und Schriftverkehr nur noch dann über die Knappschaftsältesten abzuwickeln, wenn die Versicherten sich hiermit ausdrücklich schriftlich einverstanden erklärt haben. Das bisherige Verfahren kann dazu führen, daß Knappschaftsältesten von Sozialdaten Kenntnis erhalten, obwohl dies nicht erforderlich ist. Auf die Darstellung eines ähnlich gelagerten Problems im Zusammenhang mit Versichertenältesten bei der Bundesversicherungsanstalt für Angestellte in meinem Elften Tätigkeitsbericht S. 57 weise ich hin.

Die Bundesknappschaft hat eine entsprechende Prüfung zugesagt.

11.5 Datenschutzrechtliche Verantwortlichkeit bei besonderen Organisationsformen von Sozialversicherungsträgern

Bei der von mir im Jahre 1988 durchgeführten Kontrolle der Landwirtschaftlichen Alterskasse Hessen-Nassau hatten sich wegen der dort bestehenden Verwaltungsgemeinschaft mit der Landwirtschaftlichen Berufsgenossenschaft und der Landwirtschaftlichen Krankenkasse besondere Probleme im Hinblick auf die Verantwortlichkeit für vorgenommene Datenspeicherungen und die Eingriffsberechtigung auf dort geführte Dateien gezeigt (vgl. 11. TB S. 57, 58). Im Anschluß daran hatte ich dem Bundesminister für Arbeit und Sozialordnung (BMA) empfohlen, diese Probleme auch für andere, ähnlich organisierte Sozialversicherungsträger zu prüfen und datenschutzgerecht zu lösen. Die inzwischen mit dem BMA schriftlich und mündlich geführten Erörterungen haben zu folgenden einvernehmlichen Ergebnissen geführt:

Sozialversicherungsträger, bei denen *eine* juristische Person Aufgaben verschiedener Zweige der Sozialversicherung wahrzunehmen hat — Beispiele sind die LVA Oldenburg-Bremen als Träger der *Künstlersozialversicherung* und die *Bundesknappschaft* — sind speichernde Stellen für sämtliche in ihrem Einflußbereich gespeicherten und verarbeiteten personenbezogenen Daten; die Weiterleitung von Daten innerhalb des Versicherungsträgers ist keine Datenübermittlung im Sinne des Bundesdatenschutzgesetzes. Gleichwohl ist es erforderlich zur Wahrung des Sozialgeheimnisses, die jeweiligen Zugriffsrechte und -möglichkeiten strikt funktionsbezogen auf das zur Aufgabenerfüllung jeweils Erforderliche zu beschränken. Diese Auffassung ist inzwischen durch die im Zuge der Rentenreform durchgeführte Ergänzung des § 35 SGB I bestätigt worden.

Für Sozialversicherungsträger, die in einer „Verwaltungsgemeinschaft" zusammengeschlossen sind und bei denen *mehrere* juristische Personen ggf. mehrere Zweige der Sozialversicherung betreuen, — Beispiele sind die *Sozialversicherung der Seeleute* und die *Landwirtschaftliche Sozialversicherung* — können sich hinsichtlich der Befugnis zu gemeinsamer Dateiführung und der Befugnis des Organwalters eines Versicherungsträgers, für den anderen Versicherungsträger zu handeln, nach dem geltenden Recht Besonderheiten ergeben.

So folgt für die *Landwirtschaftliche Sozialversicherung* aus der gesetzlichen Pflicht zur Zusammenarbeit, daß die drei Versicherungsträger — Landwirtschaftliche Krankenkassen, Alterskassen und Berufsgenossenschaften — gemeinsame Dateien über personenbezogene Daten ihrer Versicherten führen dürfen, soweit Daten auch zur Aufgabenerfüllung des jeweils anderen Trägers erforderlich sind. Aus dem Zusammenarbeitsgebot ergibt sich ferner, daß der gemeinsame Geschäftsführer der drei Versicherungsträger aus Zweckmäßigkeitsgründen Bedienstete eines Versicherungsträgers der Verwaltungsgemeinschaft damit betrauen kann, auch Aufgaben eines anderen Versicherungsträgers wahrzunehmen. Dementsprechend nehmen Organwalter jedes der drei Versicherungsträger in erheblichem Umfang Funktionen für andere wahr, obwohl alle drei jeweils eigenes Personal haben.

Die bei dieser engen Zusammenarbeit besonders schwierige Frage danach, wer als speichernde Stelle für die im Informationssystem der Landwirtschaftlichen Sozialversicherung (IS-LSV) gespeicherten Daten verantwortlich ist, wurde wie folgt geklärt: Für Daten, die für mehrere der drei Versicherungsträger erforderlich sind, ist jeder derartige Versicherungsträger speichernde Stelle. Bei personenbezogenen Daten, die nach § 76 SGB X nur mit Einschränkungen anderen Trägern, die diese Daten benötigen, offenbart werden dürfen — insbesondere medizinische Daten — ist nur der Träger speichernde Stelle, der dieses Datum erhalten hat. Eine gemeinsame Speicherung dieser medizinischen Daten ist unzulässig; ihre Offenbarung an einen anderen Leistungsträger der „Verwaltungsgemeinschaft", kommt nur unter den Voraussetzungen des § 76 SGB X in Betracht.

Die Geschäftsführer der Landwirtschaftlichen Sozialversicherungsträger werden eine Liste erarbeiten und zur Verfügung halten, aus der sich ergibt, welches Feld der Datenbank welchem/welchen Versicherungsträger/n der Verwaltungsgemeinschaft jeweils als speichernder Stelle zuzuordnen ist. Ist ein Feld für mehrere oder sämtliche Versicherungsträger der Verwaltungsgemeinschaft zur Erfüllung ihrer Aufgaben erforderlich, kann der betroffene Versicherte gegebenenfalls die betroffenen mehreren oder alle Versicherungsträger in Anspruch nehmen. Diese datenschutzrechtliche Haftung gleichsam „zur gesamten Hand" kommt insbesondere für die gemeinsam genutzten Einrichtungen Rechenzentrum und Teile des Verwaltungsgebäudes in Betracht. Unabhängig von der nunmehr geklärten Frage der speichernden Stelle bleibt das Erfordernis der strikt funktionsbezogen begrenzten Zugriffsberechtigung der Organwalter jedes Versicherungsträgers auf solche Datenfelder, die zur Wahrnehmung seiner Aufgaben notwendig sind, die inzwischen auch von der ausdrücklichen gesetzlichen Regelung in § 35 Abs. 1 Satz 2 SGB I gefordert wird.

Es ist beabsichtigt, die datenschutzrechtlichen Besonderheiten der Landwirtschaftlichen Sozialversicherung bei der nächsten gesetzlichen Änderung dieses Bereichs im Gesetz zu regeln.

Die Organisationsstruktur im Bereich *der Sozialversicherung der Seeleute* ist bei der See-Berufsgenossenschaft und Seekasse mit See-Krankenkasse zwar gesetzlich etwas anders gestaltet; das Nähere habe ich unter 11.2 dargestellt. Aber auch diese Sozialversicherungsträger dürfen nach den vorstehend dargelegten Grundsätzen Dateien gemeinsam führen, soweit sie für ihre Aufgabenerfüllung erforderlich sind. Für Daten, die sie gemeinsam benötigen, sind beide auch speichernde Stellen.

11.6 Offenbarung von Versichertendaten Verschollener

Im Berichtszeitraum wurde ich mit zwei Eingaben befaßt, die auf die Weigerung von Sozialversicherungs-

trägern zurückgingen, Anfragen zu beantworten, die u. a. Tatsache und Zeitpunkt des Todes sowie die letzte Anschrift von verschollenen Versicherten und deren letzte Arbeitgeber betrafen:

— Ein Amtsgericht hatte im Rahmen eines Todeserklärungsverfahrens einen Rentenversicherungsträger um Angabe der Anschrift des verschollenen Versicherten, seines Namens und der Anschrift seines letzten Arbeitgebers gebeten. Anlaß dazu war die Abwicklung einer Nachlaßangelegenheit. Der zuständige Sozialversicherungsträger hatte die im Rahmen der Amtshilfe erbetene Auskunft mit der Begründung abgelehnt, das anfragende Amtsgericht benötige die Daten nicht zur Erfüllung des gleichen Zwecks, zu dem der Sozialversicherungsträger sie erhalten habe, was § 10 BDSG voraussetze.

  Das Amtsgericht, das sich an mich wandte, hielt die Anwendung des § 10 BDSG in diesem Zusammenhang für unvereinbar mit dem Schutz der Persönlichkeitsrechte des Verschollenen, auf den §§ 67ff. SGB X abzielten.

  Das Problem läßt sich meines Erachtens wie folgt lösen:

  Ist dem Rentenversicherungsträger bekannt, daß der Verschollene verstorben ist, so kann er dem anfragenden Amtsgericht die Tatsache des Todes und das Todesdatum mitteilen. § 35 SGB I i. V. m. §§ 67ff. SGB X stehen insoweit schon deswegen nicht entgegen, weil die unmittelbare Schutzwirkung des Sozialgeheimnisses mit dem Tod endet. Eine Vorschrift wie in § 203 Abs. 4 StGB, wonach Privatgeheimnisse gegen unbefugte Offenbarung auch noch nach dem Tode des Betroffenen geschützt sind, fehlt in den bereichsspezifischen Regelungen des Sozialgesetzbuchs. Unmittelbar auf Grund der Verfassung ist aber „die *Fortwirkung* eines Persönlichkeitsrechts nach dem Tode zu verneinen, weil Träger dieses Grundrechts nur die lebende Person ist; mit ihrem Tode erlischt der Schutz aus diesem Grundrecht" (BVerfGE 30, 173, 194).

  Der Bundesminister für Arbeit und Sozialordnung hatte bereits 1986 in einem Schreiben klargestellt, daß die Mitteilung von Tod und Todesdatum eines Versicherten dem nachwirkenden Schutz des Sozialgeheimnisses nicht unterliegen. Ich habe die betroffenen Stellen auf diesen Erlaß hingewiesen und meine zustimmende Auffassung im einzelnen begründet.

  Auch die Offenbarung der letzten Anschrift des Versicherten und der Anschrift seines letzten Arbeitgebers durch den Rentenversicherungsträger halte ich in diesem Fall für zulässig. Beide Daten sind zwar noch zu Lebzeiten des verstorbenen Versicherten entstanden. Die §§ 35 SGB I i. V. m. §§ 76ff. SGB X sind aber auch auf solche Daten nach dem Tod eines Trägers von Daten, die dem Sozialgeheimnis unterlagen, nicht mehr anwendbar. Gleichwohl ist ein Verstorbener nicht völlig schutzlos. Das Bundesverfassungsgericht hat im Volkszählungsurteil das Recht auf informationelle Selbstbestimmung nicht nur als Persönlichkeitsrecht aus Artikel 2 des Grundgesetzes, sondern auch aus dem Gebot der Unverletzlichkeit der Menschenwürde des Artikel 1 Abs. 1 Grundgesetz abgeleitet. Die hieraus resultierende Schutzwirkung endet im Gegensatz zu der aus Artikel 2 GG nicht mit dem Tode (vgl. BVerfGE a. a. O.). Sie umfaßt demnach grundsätzlich auch Sozialdaten eines Verstorbenen über seien Tod hinaus, soweit deren Offenbarung geeignet ist, die Menschenwürde des Verstorbenen zu verletzen. Es ist aber in aller Regel nicht ersichtlich, daß die Offenbarung der letzten Anschrift und des letzten Arbeitgebers die Menschenwürde eines Verstorbenen beeinträchtigen könnte.

  Lebt der Verschollene noch und ist dem Versicherungsträger auch seine Anschrift bekannt, ergeben sich mehrere Lösungsmöglichkeiten: Soweit die Voraussetzungen des § 68 SGB X vorliegen, kann die Anschrift im Rahmen der Amtshilfe offenbart werden. Bei Anfragen von Privatpersonen sollte der Versicherungsträger den Versicherten über die vorliegende Anfrage informieren und ihm anheimstellen, entweder in die Offenbarung einzuwilligen, oder sich selbst zu melden. Dieses Verfahren praktiziert z. B. die BfA seit längerem.

— In einem anderen Fall hatte ein Enkel den vermuteten Rentenversicherungsträger seines Großvaters um Auskunft u. a. über das Bestehen eines Versicherungsverhältnisses, das Todesdatum und die letzte Anschrift sowie darüber gebeten, ob der Großvater wieder geheiratet habe. Das Auskunftsersuchen wurde mit dem Interesse daran begründet, etwaige Nachkommen aus einer möglichen zweiten Ehe des Großvaters zu finden, der vor Kriegsende in den Vertreibungsgebieten gelebt hatte. Die Versicherungsanstalt der ehemaligen Dienstbehörde des Großvaters hatte die erbetenen Auskünfte unter Berufung auf § 35 SGB I i. V. m. §§ 67ff. SGB X insgesamt verweigert.

  Im vorliegenden Falle halte ich eine eingeschränkte Offenbarung für zulässig. Der Offenbarung der Tatsache des Todes, des Todesdatums und — falls bekannt — der letzten Anschrift des verstorbenen Großvaters stehen nach den vorstehend entwickelten Grundsätzen datenschutzrechtliche Bedenken nicht entgegen.

  Ob eine Offenbarungsbefugnis im Hinblick auf eine mögliche Eheschließung des Großvaters besteht, müßte unter Berücksichtigung aller Umstände des Einzelfalles entschieden werden. Da eine solche nur dann ausscheidet, wenn durch die Offenbarung die Würde des Verstorbenen verletzt würde, wird auch über dieses Datum in aller Regel Auskunft gegeben werden können.

11.7 Kinder- und Jugendhilfegesetz

Gegen den Entwurf des Kinder- und Jugendhilfegesetzes (KJHG), mit dem u. a. das Jugendwohlfahrtsgesetz abgelöst werden soll, bestehen aus der Sicht des Datenschutzes zwar keine grundsätzlichen Bedenken. Es fehlen jedoch normenklare Regelungen über

Befugnisse zur Erhebung, Speicherung, Löschung, Auswertung und Weitergabe personenbezogener Daten sowie organisatorische Regelungen, die bei der Datenverarbeitung die erforderliche klare Abgrenzung der unterschiedlichen Aufgaben der Jugendhilfe ermöglichen. Ich habe dem BMJFFG im einzelnen folgende Ergänzungen vorgeschlagen:

— Wie im Gesundheitsreformgesetz (vgl. §§ 284ff. SGB V) und im Rentenreformgesetz (vgl. §§ 148ff. SGB VI) sollte ein eigenes Kapitel über die Informationsgrundlagen der Jugendhilfe, die Speicherungszwecke, Offenbarung und Löschung von personenbezogenen Daten geschaffen werden.

— Die Auskunftspflichten der Beteiligten und Dritter (z. B. Arbeitgeber) sind im Gesetz möglichst präzise aufzuführen.

— Es sollten Regelungen getroffenen werden, die die Persönlichkeitsrechte von Personen aus dem sozialen Umfeld von Minderjährigen bei Akteneinsicht und Auskünften angemessen schützen.

— Der Gesetzentwurf muß sicherstellen, daß Erkenntnisse aus der Beratungstätigkeit nicht bei der sonstigen Aufgabenerfüllung der Jugendämter verwertet und möglicherweise gegen die Beratenen verwendet werden.

In einer ersten Besprechung mit dem BMJFFG, an der u. a. auch der Bundesminister für Arbeit beteiligt war, wurde grundsätzliche Übereinstimmung darüber erzielt, daß datenschutzrechtliche Bestimmungen noch im Verlaufe des Gesetzgebungsverfahrens in den Entwurf eingefügt werden sollen.

12 Arbeitsverwaltung

12.1 Kontrollen von Arbeitsämtern

Im Laufe des Berichtsjahres habe ich mehrere Beratungsgespräche mit Vertretern der Bundesanstalt für Arbeit (BA) sowohl auf regionaler Ebene bei Arbeitsämtern als auch in der Hauptstelle in Nürnberg geführt.

— Aufgrund einer Eingabe habe ich mich mit der Problematik der Behandlung *anonym eingegangener Anzeigen* von Leistungsmißbrauchstatbeständen durch die BA befaßt. Die aus diesem Anlaß im betreffenden Arbeitsamt durchgeführte Kontrolle hat folgende Praxis gezeigt: Anonyme Anzeigen werden vom Arbeitsamt — soweit sie sich einem bestimmten Leistungsempfänger zuordnen lassen — zu dessen Leistungsakte genommen. Das Arbeitsamt ermittelt sodann, ob ein bußgeldpflichtiger oder strafbarer Leistungsmißbrauchstatbestand vorliegt. Auch dann, wenn die durchgeführten Ermittlungen keinerlei Verdachtsmomente für einen Leistungsmißbrauch ergeben, wird der anonyme Hinweis mit der Begründung, es könnten noch weitere Anzeigen in gleicher Sache eingehen, die eine Chance zur späteren Aufklärung böten, bei der Leistungsakte belassen. Darüber hinaus läßt es nach Auffassung der BA das Prinzip der Vollständigkeit der Akten nicht zu, rechtmäßig zu den Akten gelangte Vorgänge zu entfernen.

Ich vertrete dazu folgende Auffassung: Soweit die Kenntnis personenbezogener Daten zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben nicht mehr erforderlich ist, sind die Daten zu löschen. Anonymen Anzeigen ist in diesem Zusammenhang möglichst unverzüglich nachzugehen. Soweit die Ermittlungen der Behörde den Inhalt bestätigen oder hinreichend konkrete Verdachtsmomente für eine Ordnungswidrigkeit oder Straftat des Betroffenen Anlaß zu weiteren Nachprüfungen geben, kann die Anzeige zur Akte des Betroffenen genommen werden. Anzeigen, deren Inhalt sich dagegen als falsch oder nicht erweisbar herausstellt, sind zu vernichten. Ihre Aufbewahrung könnte den Betroffenen auch in Zukunft zu Unrecht belasten.

Ich habe hiernach im konkreten Fall die Aufbewahrung einer anonymen Anzeige in der Leistungsakte als Verstoß gegen den u. a. in § 84 SGB X zum Ausdruck gebrachten Grundsatz, daß personenbezogene Daten zu löschen sind, falls und soweit ihre Kenntnis für die Aufgabenerledigung der speichernden Stelle nicht mehr erforderlich ist, beanstandet. Zu dieser Entscheidung hat beigetragen, daß bei dem betroffenen Arbeitsamt noch ein weiterer Verstoß gegen den Grundsatz, daß nur erforderliche Daten gespeichert werden dürfen, festgestellt worden war.

— Bereits im Elften Tätigkeitsbericht (S. 52/53) hatte ich mich mit der *Gestaltung der Publikumszonen* in den Dienststellen der Bundesanstalt für Arbeit (BA) beschäftigt. Bei der Kontrolle eines Arbeitsamtes habe ich hierzu erneut datenschutzrechtliche Probleme festgestellt. In diesem Arbeitsamt haben sich Besucher der Abteilung Arbeitsvermittlung/Arbeitsberatung zunächst in der Anmelde- und Bearbeitungsstelle zu melden. Dort werden ihre Anliegen vorgeklärt; sie werden beim Ausfüllen von Anmeldebögen und Antragsvordrucken unterstützt und ggf. zu der zuständigen Beratungsfachkraft weitergeleitet. Die Anmelde- und Bearbeitungsstellen sind im Arbeitsamt selbst und in der Nebenstelle in der Regel mit drei bis vier Mitarbeitern besetzt und in zwei, teilweise durch eine Zwischentür verbundenen Zimmern untergebracht. Bei großem Andrang wird an beiden Schreibtischen je Zimmer gleichzeitig Publikumsverkehr abgewickelt.

Meine Mitarbeiter konnten sich davon überzeugen, daß am Nachbartisch geführte Gespräche von unbeteiligten Besuchern mitgehört werden konnten. Inhalt der Gespräche waren u. a. sensible persönliche Daten, wie Familienstand, Krankheitszeiten und Bezug von Sozialleistungen. Dritten war auch eine unbefugte Einsichtnahme in von Besuchern vorgelegte Unterlagen ohne besondere Anstrengung möglich.

Ich habe diese Organisation und Unterbringung der Anmelde- und Bearbeitungsstellen als Verletzung des Sozialgeheimnisses gemäß § 35 Sozialgesetzbuch (SGB I) i. V. m. §§ 67ff. SGB X beanstan-

det. Der Bundesanstalt für Arbeit wurde nochmals dringend empfohlen, ihre Richtlinien für die räumliche Unterbringung der Anmelde- und Bearbeitungsstellen sowie die Möglichkeiten weitergehender Schutzvorkehrungen gegen ein unbefugtes Mithören und Mitlesen Dritter zu überprüfen. Die BA hat mir daraufhin mitgeteilt, eine generelle Einzelzimmerunterbringung der Mitarbeiter in den Anmelde- und Bearbeitungsstellen halte sie im Hinblick auf den weniger sensiblen Gehalt der erörterten Daten für einen unverhältnismäßig hohen Aufwand. Sie kündigte an, daß die erforderliche Vertraulichkeit durch Trennwände und abschirmende Grünpflanzen sichergestellt werden soll. Ich habe Zweifel, ob diese Planung meinem Anliegen gerecht wird und werde mich von der Wirksamkeit der Maßnahmen überzeugen.

— Im Rahmen einer Kontrolle habe ich im *Verfahren der computerunterstützten Arbeitsvermittlung (coArb)* der Bundesanstalt für Arbeit (s. auch 10. TB S. 63). folgende Zugriffsmöglichkeiten von Mitarbeitern der Abteilung Arbeitsvermittlung/Arbeitsberatung auf automatisiert gespeicherte Daten festgestellt: Die Vermittlungsfachkräfte (Hauptvermittler, Arbeitsberater) haben lesenden und verändernden Zugriff auf die coArb-Daten aller gegenwärtigen und früheren Arbeitslosen des jeweiligen Arbeitsamtsbezirks, in der Regel noch bis zu vier Monate nach Beendigung der Arbeitslosigkeit. Alle Mitarbeiter der Anmelde- und Bearbeitungsstellen haben lesenden, ein bis zwei Mitarbeiter darüber hinaus verändernden Zugriff auf die oben genannten coArb-Daten.

Die Notwendigkeit dieser Zugriffsmöglichkeiten wird durch die Bundesanstalt für Arbeit u. a. mit zunehmenden „Unschärfen" am Arbeitsmarkt hinsichtlich des Herkunftsberufes des Bewerbers und der Anforderungsprofile der zu besetzenden Stellen sowie der Möglichkeit des verbesserten regionalen Ausgleichs innerhalb des Hauptamtes und der Nebenstellen begründet.

Ich habe darauf hingewiesen, daß der Grundsatz des Sozialgeheimnisses gemäß § 35 SGB I die Sozialleistungsträger verpflichtet, personenbezogene Daten auch intern nur in dem Umfang zugänglich zu machen, in dem die Kenntnis zur Aufgabenerledigung der jeweiligen Mitarbeiter unbedingt erforderlich ist. Weitergehende Zugriffsmöglichkeiten begründen die Gefahr einer Verletzung des Sozialgeheimnisses. Die Bundesanstalt für Arbeit sieht dieses Risiko offenbar im Grundsatz auch. So werden z. B. die Bewerberdaten der eigenen Mitarbeiter, die zuvor arbeitslos gemeldet waren, nach Maßgabe eines entsprechenden Erlasses unverzüglich nach Beendigung ihrer Arbeitslosigkeit gelöscht.

Ich habe schon deshalb Zweifel an der Erforderlichkeit der bisher eingeräumten Zugriffsmöglichkeit auf alle coArb-Daten, weil nach der organisatorischen Zuständigkeitsregelung innerhalb der Abteilung Arbeitsvermittlung/Arbeitsberatung die einzelne Vermittlungsfachkraft sowie die Anmelde- und Bearbeitungsstelle jeweils nur für bestimmte Berufsgruppen zuständig ist. Da der Arbeitssuchende somit im Regelfall von bestimmten für seine Berufsgruppe zuständigen Mitarbeitern betreut wird, dürfte ein Zugriff auf personenbezogene Daten innerhalb des jeweiligen Zuständigkeitsbereichs eines Mitarbeiters in der Regel ausreichen. Soweit im Einzelfall eine Mitbetreuung durch weitere Vermittlungsfachkräfte erforderlich erscheint, dürfte es genügen, den weiteren Mitarbeiter der Bundesanstalt für Arbeit persönlich einzuschalten oder eine auf den jeweiligen Fall beschränkte weitergehende Zugriffsmöglichkeit einzuräumen.

Meine Auffassung ist in der Zwischenzeit durch die im Zuge der Rentenreform erfolgte Ergänzung des § 35 Abs. 1 SGB I bestätigt worden.

— Im Berichtszeitraum waren *Außenprüfungen* der BA insbesondere unter dem Gesichtspunkt der Erforderlichkeit der erhobenen personenbezogenen Daten für die Aufgabenerledigung der BA Gegenstand einiger Eingaben. Ich habe der BA gegenüber angeregt, bei systematischen Prüfungen den Umfang der Datenerhebung im Sinne des Verhältnismäßigkeitsprinzips auf das wirklich Erforderliche zu beschränken. Das kann es nahelegen, bei systematischen Prüfungen grundsätzlich zunächst nur Stichprobenprüfungen vorzusehen und dann auf Grund der gewonnenen Erfahrungen gezielt unter bestimmten Gesichtspunkten, die Indizien für Mißbräuche sein können, weiter zu prüfen. Außenprüfungen, bei denen die personenbezogenen Daten aller Arbeitnehmer des Betriebes erhoben werden, sollten nur in Ausnahmefällen durchgeführt werden.

Ich bin überzeugt, daß eine solche Regelung nicht nur ein Beitrag für einen verbesserten Datenschutz, sondern auch für eine wirksamere und effizientere Prüfpraxis sein könnte. Die BA beabsichtigt, die bestehende Weisung für die Durchführung von Außenprüfungen anläßlich der Neufassung des § 132 a AFG durch das Gesetz zur Einführung des Sozialversicherungsausweises zu überarbeiten. Die BA hat mir zugesagt, mich an der Neufassung zu beteiligen.

In einem einer Eingabe zugrundeliegenden Fall hat die BA die Außenprüfung so durchgeführt, daß sie die Daten einer bestimmten großen Gruppe von Mitarbeitern eines Betriebes erhoben und anschließend mit den Datenbeständen der BA automatisiert abgeglichen hat. Dieses Verfahren ist rechtlich problematisch. Außenprüfungen nach § 132 a Abs. 1 AFG beschränken sich auf Ermittlungen zur Feststellung, ob für den Betrieb Arbeitnehmer und Selbständige während einer Zeit tätig sind oder tätig waren, für die sie Arbeitslosengeld beantragt haben, beziehen oder bezogen haben und darauf, ob die Angaben in der Arbeitsbescheinigung nach § 133 AFG zutreffend bescheinigt sind. Die BA ist insoweit u. a. berechtigt, Geschäftsbücher und Geschäftsunterlagen einzusehen. § 132 a AFG kann nicht ohne weiteres entnommen werden, daß auch ein automatisierter Abgleich von Datenbeständen, wie er bei der erwähnten Außenprüfung vorgenommen worden ist, zulässig sein soll. Bei einem solchen Verfahren wer-

den überwiegend Daten von Personen verarbeitet, die selbst nicht verdächtig sind. Es bedarf deshalb einer besonderen gesetzlichen Grundlage, die die Anwendung begrenzt und Sicherungen vorsieht. So soll z. B. nach dem Entwurf eines Strafverfahrensänderungsgesetzes der Datenabgleich im Strafverfahren in neuen §§ 98 a und 98 b StPO geregelt und nur sehr eingeschränkt auf richterliche Anordnung zugelassen werden. Nach dem gleichen Entwurf soll eine Offenbarung von Daten, die dem Sozialgeheimnis unterliegen, für Zwecke einer Rasterfahndung nach den genannten Vorschriften der StPO unzulässig sein.

Aus diesen Gründen habe ich den BMA gebeten zu prüfen, ob im Zusammenhang mit Außenprüfungen der BA derartige Datenabgleiche zur Bekämpfung von Schwarzarbeit und Leistungsmißbrauch unbedingt erforderlich sind. Für diesen Fall habe ich dringend empfohlen, möglichst rasch eine normenklare gesetzliche Regelung mit den entsprechenden Beschränkungen und Sicherungen zu schaffen. Gleichzeitig sollten Bestimmungen über Art und Umfang der bei Außenprüfungen zu erhebenden Daten, die der Bundesanstalt zustehenden Befugnisse sowie die Rechte betroffener Personen geschaffen werden.

— Auf Grund einer Einzeleingabe habe ich bei einem Arbeitsamt die *Aufbewahrung von ärztlichen Gutachten* kontrolliert. Hierbei stellte ich fest, daß sich in mehreren Fällen in den Vermittlungsunterlagen ärztliche Gutachten mit detaillierten Diagnose- oder Anamnesedaten befanden, die nach Auffassung der mit der Arbeitsvermittlung betrauten Mitarbeiter überwiegend für ihre Arbeit nicht benötigt wurden, beispielsweise ein 1983 erstelltes ärztliches Gutachten, dessen Aussagewert ausdrücklich auf ein Jahr beschränkt war.

Ich habe die Aufbewahrung als Verstoß gegen § 9 BDSG, § 84 SGB X sowie gegen den Grundsatz der internen Vertraulichkeit von Gesundheitsdaten beanstandet und empfohlen, in den Vermittlungsunterlagen lediglich die in den ärztlichen Gutachten gegebenen Hinweise auf etwaige Einschränkungen der beruflichen Verwendungsfähigkeit und/oder entsprechende Verwendungsvorschläge zu speichern. Ärztliche Gutachten sollten nur entsprechend dem für psychologische Gutachten vorgesehenen Verfahren (s. 11. TB S. 94 Nr. 27) bei der Vermittlungsabteilung aufbewahrt werden. Um die Aufbewahrung ärztlicher Gutachten durch die Vermittlungsabteilung über deren medizinische Aussagefähigkeit hinaus von vornherein auszuschließen, sollte der Ärztliche Dienst bereits im Gutachten selbst einen Hinweis auf die voraussichtliche Dauer der Aussagefähigkeit des Gutachtens geben. Mit Ablauf dieser Frist sollte das Gutachten vernichtet werden. Eine Rückgabe an den Ärztlichen Dienst erscheint wegen der dort vorhandenen Kopien nicht erforderlich.

Die Hauptstelle der Bundesanstalt für Arbeit hält demgegenüber diagnostische und anamnestische Feststellungen unabhängig davon, wann sie getroffen wurden, für die Beurteilung relevanter Gesundheitsstörungen des Arbeitssuchenden durch die jeweilige Vermittlungsfachkraft für erforderlich. Nach ihrer Auffassung ist eine allgemeine Festlegung der Gültigkeitsdauer ärztlicher Gutachten nicht möglich. Der Arbeitsberater/Hauptvermittler habe vielmehr im Einzelfall zu entscheiden, ob eine erneute Begutachtung aufgrund mangelnder Aktualität einzelner Befunde erforderlich sei. Die hiermit verbundene Verlagerung der ärztlichen Entscheidungskompetenz auf Nichtfachleute halte ich für eine wenig überzeugende Alternative zu dem von mir vorgeschlagenen Verfahren.

Ich werde mich weiterhin für eine sach- und damit auch datenschutzgerechtere Verfahrensweise einsetzen.

12.2 Nachweispflicht im Leistungsverfahren

In meinem Elften Tätigkeitsbericht hatte ich mich mit der Frage beschäftigt, inwieweit die Bundesanstalt für Arbeit Unterlagen, die zur Einkommensermittlung von dem Arbeitslosen und den Angehörigen vorgelegt werden (z. B. Rentenbescheide; Verträge, aus denen Einkommen erwächst usw.), zur Akte nehmen darf. Die Bundesanstalt für Arbeit hat das Verfahren nunmehr wie folgt geregelt:

Unterlagen, die ihrem Typ nach leicht auszuwerten sind (z. B. Rentenbescheide, Lebens-, Haftpflichtversicherungspolicen usw.), sind vom Antragsannehmer nach Bestätigung der Übereinstimmung mit der im Vordruck erfolgten Eintragung durch Handzeichen sofort zurückzugeben. In den übrigen Fällen sollen nach Entscheidung über den Leistungsantrag grundsätzlich nur diejenigen Unterlagen (in Ablichtung) in der Leistungsakte bleiben, die nicht schon in sich plausible Feststellungen (z. B. erheblich voneinander abweichende Angaben in verschiedenen Unterlagen) betreffen. In diesen Fällen sind personenbezogene Daten unbeteiligter Personen, deren Identität für die Entscheidung und eine etwaige spätere Überprüfung des Leistungsfalles unerheblich ist, zu schwärzen.

Darüber hinaus habe ich mich mit der Frage befaßt, welche Unterlagen Unterhaltsverpflichtete, die z. B. im Verfahren der Gewährung von Arbeitslosenhilfe ihre Leistungsfähigkeit anerkennen, vorzulegen haben. Eine Besprechung der Problematik mit dem Bundesminister für Arbeit und Sozialordnung erbrachte u. a. folgende Ergebnisse:

— Die Bundesanstalt für Arbeit wird auf die genaue Ermittlung des Einkommens eines unterhaltsverpflichteten Angehörigen künftig verzichten, wenn dieser durch einen Steuerbescheid oder eine Bescheinigung seines Steuerberaters darlegt, daß aufgrund der Höhe seines Einkommens Arbeitslosenhilfe an den Unterhaltsberechtigten nicht zu zahlen ist.

— Soweit die Arbeitslosmeldung lediglich dem Ziel dient, die Zeit der Arbeitslosigkeit gemäß § 1259 RVO als Ausfallzeit für die Rentenversicherung angerechnet zu bekommen, kann nunmehr auf eine formelle Antragstellung verzichtet werden, wenn anhand der vorgelegten Nachweise (z. B.

Lohn- oder Gehaltsbescheinigung, Rentenbescheide, vom Finanzamt bestätigte Erklärungen) eindeutig erkennbar ist, daß eine Leistungsgewährung wegen fehlender Bedürftigkeit oder Anrechnung einer Abfindung nicht in Betracht kommt. Die Bundesanstalt für Arbeit wird diese Information in die Neuauflage des Merkblatts für Arbeitslose ab April 1990 aufnehmen.

Diese Regelungen enthalten einen erfreulichen datenschutzrechtlichen Fortschritt.

12.3 Verfahren bei der Gewährung von Arbeitslosenhilfe

Häufig beschweren sich Unterhaltspflichtige darüber, daß ihr genaues Einkommen im Rahmen der Leistungsgewährung dem Antragsteller bekannt wird (s. 12.2). Ich habe bereits in früheren Tätigkeitsberichten (10. TB S. 64, 9. TB S. 49) zu diesem Problem Stellung genommen. Der Bundesminister für Arbeit und Sozialordnung teilt allerdings nicht meine bereits früher dargestellte Auffassung, daß im Interesse einer Wahrung der Vertraulichkeit der Einkommensverhältnisse der Unterhaltsverpflichteten die Angabe des Anrechnungsbetrages im Bewilligungsbescheid ausreicht und weitere Angaben erst im Widerspruchsverfahren erforderlich werden. Er verweist u. a. auf das Begründungserfordernis für Verwaltungsakte aus § 35 Abs. 1 SGB X sowie die Auskunftspflicht Unterhaltspflichtiger gemäß § 1605 BGB.

Das derzeitige Verfahren der Anrechnung fiktiver Unterhaltsansprüche gemäß § 137 Arbeitsförderungsgesetz (AFG) soll in einer Übergangsvorschrift geregelt werden, die bis zum 31. Dezember 1992 gelten soll. Ich werde mich in diesem Zusammenhang weiterhin für eine datenschutzgerechtere Verfahrensweise einsetzen.

12.4 Arbeitsverwaltung — Einzelfälle

- Bereits in früheren Tätigkeitsberichten habe ich mich mit der Problematik der *Angabe des Zahlungsgrundes* (Art, Höhe und Zeitraum einer Sozialleistung) *auf den Überweisungsbelegen* der Bundesanstalt für Arbeit beschäftigt (s. 4. TB S. 19; 5. TB S. 58). Die Bundesanstalt für Arbeit sieht die Angabe nach wie vor aus Gründen des Pfändungsschutzes gemäß § 55 SGB I und der besseren Identifizierbarkeit der Überweisung durch den Empfänger als erforderlich an. Auf meine Anregung hin hat sie jedoch den zentralen Kreditausschuß der Deutschen Bundesbank auf die besonderen Verwendungsbeschränkungen bei Sozialleistungen gemäß § 78 SGB X hingewiesen. Dieser hat das Schreiben an die Spitzenverbände des Kreditgewerbes weitergeleitet, die die angeschlossenen Kreditinstitute unterrichten werden. Ich gehe davon aus, daß diese Informationen dazu beitragen, die Wahrung des Sozialgeheimnisses auch bei den Kreditinstituten zu sichern.

- Das Institut für Arbeitsmarkt- und Berufsforschung der Bundesanstalt für Arbeit schrieb im Rahmen einer Untersuchung die Empfänger von Überbrückungsgeld mit der Bitte an, einen Erhebungsbogen mit Fragen zur geförderten Existenzgründung zu beantworten. Obwohl eine anonymisierte Auswertung zugesichert wurde, ließen einige Erhebungsbogen die Anschrift des Betroffenen, die sich beim Ausfüllen des Adressenfeldes des Anschreibens durchgedrückt hatte, erkennen. Die Bundesanstalt für Arbeit hat auf meine Bitte die auf die angegebene Weise identifizierbaren Erhebungsbögen gegen anonymisierte ausgetauscht.

- Durch eine Eingabe wurde mir ein *Vordruck zur Entbindung von der ärztlichen Schweigepflicht* bekannt, der von der Arbeitsverwaltung Nordrhein-Westfalen im Rahmen der Bewilligung von Kindergeld verwendet wird. Auf der Grundlage dieses Vordruckes sollen Ärzte in bestimmten Fällen von der Schweigepflicht entbunden werden, um es dem Ärztlichen Dienst des Arbeitsamtes zu ermöglichen, mit dem behandelnden Arzt des Kindes Kontakt aufzunehmen und sich erforderlichenfalls die zur Klärung entscheidungserheblicher Fragen notwendigen ärztlichen Unterlagen übersenden zu lassen. Dadurch soll insbesondere eine erneute Untersuchung des Kindes vermieden werden. Ich habe angeregt, die Erklärung zur Entbindung von der Schweigepflicht datenschutzfreundlicher zu gestalten. Die Arbeitsverwaltung hat den Vordruck zwischenzeitlich überarbeitet und neu aufgelegt. Er enthält nunmehr u. a. die Angabe des Zweckes der Datenverwendung sowie die genaue Bezeichnung des Arztes, der von der Schweigepflicht entbunden wird.

- Ein Petent wandte sich gegen das *namentliche Aufrufverfahren,* das *in der Antragsannahmestelle der Leistungsabteilung* eines Arbeitsamtes praktiziert wurde, wodurch allen Wartenden die Namen der Arbeitslosen bekannt wurden. Ich habe diese Verfahrensweise gemäß § 20 Abs. 1 BDSG als Verstoß gegen das Sozialgeheimnis nach § 35 Sozialgesetzbuch (SGB I) beanstandet. Den Verantwortlichen war schon länger bekannt gewesen, daß das praktizierte namentliche Aufrufverfahren gegen das Sozialgeheimnis verstößt. Sie hatten nichts dagegen unternommen, obwohl die Möglichkeit bestand, das Verfahren auf ein Nummernsystem umzustellen. Inzwischen wurde im gesamten Zuständigkeitsbereich des betroffenen Landesarbeitsamtes ein datenschutzgerechtes Wartenummern-Aufrufverfahren eingeführt. Ich begrüße diese Entscheidung.

- Ein Arbeitsamt hatte ein Meldeversäumnis im Sinne des § 120 AFG mit der Begründung festgestellt, die vorgelegte Bescheinigung der Ärztin könne als sog. „Gefälligkeitsattest" die unterbliebene Vorsprache der Petentin nicht entschuldigen. Im anschließenden Verfahren vor dem Sozialgericht führte das Arbeitsamt zur Unterstützung seiner Auffassung die *Namen weiterer Leistungsbezieher*, die ebenfalls bei Meldeversäumnissen ärztliche Atteste dieser Ärztin vorgelegt hatten, in das Verfahren ein. Ich habe die Bekanntgabe der Namen anderer Leistungsempfänger in dem Verfahren als Verstoß gegen das Sozialgeheimnis im

Sinne des § 35 SGB I gewertet. Eine Offenbarung der Namen war zur Erfüllung sozialer Aufgaben der Bundesanstalt für Arbeit nicht erforderlich; es hätte vielmehr ausgereicht, im Rahmen der Abgabe einer Hintergrundinformation weitere Atteste der Ärztin anonymisiert zu bezeichnen. Die Bundesanstalt für Arbeit hat eingeräumt, daß die volle Namensnennung weiterer Leistungsbezieher im Rahmen der Aufgabenerfüllung des Arbeitsamtes nicht erforderlich war und gegen § 35 SGB I verstieß. Sie wird den Eingabesachverhalt zum Anlaß nehmen, nochmals auf die gesetzlich eng begrenzte Offenbarungsbefugnis auch in derartigen Fällen hinzuweisen.

— Aufgrund einer Pressemitteilung wurde mir bekannt, daß bei *Ausbildungsplätzen*, die Arbeitsämter im Rahmen der Berufsberatung vermitteln, auf Wunsch der ausbildungswilligen Betriebe Hinweise wie „Keine Ausländer", „Nur Deutsche" u. ä. in das Datenverarbeitungsverfahren der BA aufgenommen werden. Da dies zu nicht erforderlichen Datenerhebungen führen kann, habe ich mich an die BA gewandt.

Die BA hat mir auf meine Anfrage hin mitgeteilt, daß das Verfahren durch bundesweit geltende Weisungen für die Zukunft wie folgt geregelt worden ist: Die Berufsberater/Ausbildungsstellenvermittler der Arbeitsämter werden Betriebe, die bei Ausbildungsstellenangeboten die Einstellung von Bewerbern bestimmter Nationalitäten ausschließen, auf die Unzulässigkeit dieser Einschränkung hinweisen. Beharrt der Betrieb trotz entsprechender Belehrung auf seiner Einschränkung, wird das Stellenangebot zurückgewiesen. Eine Speicherung des Datums „Keine Ausländer" o. ä. auf Ausbildungsstellenangeboten ist danach künftig ausgeschlossen.

13 Krankenversicherung

13.1 Gesundheits-Reformgesetz — Erste Erfahrungen —

In meinem letzten Tätigkeitsbericht habe ich über die datenschutzrechtlichen Aspekte und Verbesserungen des Gesundheits-Reformgesetzes berichtet (S. 55/56). Die in dieses Gesetz unter meiner Mitarbeit aufgenommenen Datenschutzregelungen haben dazu geführt, daß inzwischen ähnliche bereichsspezifische Vorschriften in das Rentenreformgesetz eingearbeitet worden sind (s. 14.1). Eine ähnliche Ergänzung des Entwurfs eines Kinder- und Jugendhilfegesetzes wird auf meine Anregung hin gegenwärtig erörtert (s. 11.7).

Ich habe das Gesundheits-Reformgesetz letztlich als „datenschutzrechtlich in Ordnung" bewertet, aber auch verschiedentlich betont, daß es — wie jedes andere Gesetz — erst durch die Praxis mit Leben erfüllt werden muß. An dieser Auffassung halte ich fest.

Ob die Praxis datenschutzfreundlich gestaltet wird, hängt auch von den Regelungen ab, die in den vorgesehenen Vereinbarungen zwischen den Verbänden der Krankenkassen, der Kassenärztlichen Vereinigungen und der übrigen Leistungserbringer erarbeitet werden. Deshalb verfolge ich die einschlägigen Verhandlungen mit Interesse. Meine Beratung bei der Vorbereitung solcher Vereinbarungen habe ich angeboten.

Das Gesundheits-Reformgesetz hat eine Reihe von datenschutzrechtlichen Problemen gelöst, die immer wieder aus der Praxis an mich herangetragen wurden. Dies gilt insbesondere für

— die Vorschriften der §§ 295, 301 und 302, welche die Datenübermittlung durch Ärzte und sonstige Leistungserbringer im Rahmen des Abrechnungsverfahrens erheblich präziser regeln als die vor der Gesundheitsreform geltenden Bestimmungen;

— die Festlegung eines eigenen Versichertenstatus für mitversicherte Familienangehörige, eine Regelung, die ich auch im Beihilferecht für Beamte anstrebe (s. 6.6.1);

— die Regelung des § 284 Abs. 4 SGB V, nach der Leistungsdaten, insbesondere medizinische Daten von Mitarbeitern der Krankenkassen und deren Familienangehörigen nicht mehr Vorgesetzten mit Personalentscheidungsbefugnissen zugänglich sein dürfen;

— schließlich wird in der Krankenversichertenkarte (spätestens ab 1. Januar 1992) der Versichertenstatus „Rentner" in Zukunft diskret zum Ausdruck gebracht; die auffällige Kennzeichnung auf dem bisherigen Krankenschein hat manchen Bürger gestört.

Erste Erkenntnisse über die Auswirkungen des Gesundheits-Reformgesetzes in der Praxis liegen mir aus Kontrollen von Krankenkassen und Bürgereingaben bereits vor. Während bei den kontrollierten Krankenkassen keine gravierenden Mängel in der Umsetzung festgestellt werden konnten (s. 11.2 und 13.2) und die datenschutzrechtlich besonders interessanten Vorschriften über die Stichprobenprüfung noch nicht praktiziert werden, ergaben sich grundsätzliche Fragen u. a.

— zur Auskunftspflicht über Einkommensverhältnisse gegenüber Krankenkassen im Zusammenhang mit den Härtefallregelungen nach den §§ 61 und 62 SGB V;

— zur Meldepflicht über Versorgungsbezüge einschließlich Betriebsrenten gegenüber der Krankenkasse nach Maßgabe der Neuregelungen in §§ 202, 226, 229 ff. und 256 SGB V;

— zum Verbot, ab 1. Januar 1992 die Rentenversicherungsnummer als Krankenversichertennummer zu verwenden;

— zur Weitergabe von ärztlichen Informationen an Kassenärztliche Vereinigungen und Krankenkassen und an den Medizinischen Dienst;

— zur Änderungsmitteilung an Krankenkassen bei stationärer Krankenhausbehandlung;

— zum Beratungsverfahren der Krankenkassen im Rahmen einer verbesserten Gesundheitsvorsorge.

Die meisten dieser Fragen lassen sich in der Praxis durch sinnvolle, am Gesetzeszweck ausgerichtete Auslegung lösen. Ob zu einzelnen Punkten eine gesetzliche Klarstellung angestrebt werden sollte, kann erst entschieden werden, wenn weitere Erfahrungen gewonnen worden sind, insbesondere mit den Vorschriften, die bisher noch nicht praktiziert werden konnten.

13.2 Kaufmännische Krankenkasse Hannover

Im Berichtsjahr habe ich eine datenschutzrechtliche Kontrolle der Kaufmännischen Krankenkasse Hannover (KKH) durchgeführt und festgestellt, daß die Organisation des Datenschutzes bei der geprüften Krankenkasse im allgemeinen den gesetzlichen Anforderungen entspricht. Zur Verbesserung des Datenschutzes habe ich der KKH folgende Empfehlungen gegeben:

— Die in Einzeldienstanweisungen getroffenen Regelungen des Datenschutzes und der Datensicherung sollten in ein überschaubares Datenschutzhandbuch für alle Mitarbeiter aufgenommen werden.

— Der interne Datenschutzbeauftragte sollte jährlich einen Bericht über alle datenschutzrechtlich relevanten Vorgänge erstellen, der allen Mitarbeitern zugänglich gemacht wird und der auch Hinweise für datenschutzgerechte Lösungen enthält; er sollte auch bei der Auswahl der in der automatisierten Verarbeitung personenbezogener Daten tätigen Personen beratend beteiligt werden (§ 29 Nr. 4 BDSG). Wegen der bundesweiten Organisationsstruktur der KKH und der damit verbundenen Aufgabenfülle sollten ihm zumindest auf Landesgeschäftsstellenebene Ansprechpartner für den Datenschutz zur Seite gestellt werden.

— Fehlversuche bei der Paßworteingabe sollten dokumentiert und zumindest stichprobenweise überprüft werden; auch die auftragsgemäße Programmanwendung und der datenschutzgerechte APC-Einsatz sind laufend zu überprüfen.

— Der Einsatz privateigener APC oder Homecomputer für den dienstlichen Gebrauch sollte verboten werden.

— Die Übersicht über die bei der KKH vorhandenen Dateien und den automatisiert oder noch manuell geführten Datenbestand sollte hinreichend differenziert werden und vor allem Angaben über Datenherkunft, Rechtsgrundlagen für die Datenerhebung, Speicherung, Übermittlung, Art der zu übermittelnden Daten und Zugriffsberechtigungen sowie Hinweise auf besondere Schutzwürdigkeit (z. B. bei medizinischen Daten), Verbleib und Verwendung aller Ausdrucke, Art und Umfang bestehender Auftragsdatenverarbeitung und Auftragnehmer enthalten.

— Kontrollen der Entsorgung von Datenträgern sollten vorgeschrieben werden.

Ich habe die Kontrolle auch zum Anlaß genommen, mich über die bisherige Umsetzung des Gesundheits-Reformgesetzes zu informieren (s. auch 13.1). Dabei konnte ich erfreulicherweise feststellen, daß die Vorschrift des § 284 Abs. 4 SGB V (Gesundheits-Reformgesetz) vorbildlich umgesetzt wurde: Die personenbezogenen Leistungs- und Versichertendaten der Beschäftigten der Krankenkasse und ihrer Angehörigen werden in einem eigenständigen Bereich von Mitarbeitern ohne Personalverwaltungs- und -entscheidungsaufgaben betreut.

Demgegenüber habe ich im Zusammenhang mit der Beihilfebearbeitung festgestellt, daß Personalverwaltung und Beihilfestelle in einer Einheit organisatorisch zusammengefaßt sind. Dies ist wegen der besonderen Sensibilität medizinischer Daten der betroffenen Mitarbeiter nicht vertretbar (s. 10. TB S. 27, 9. TB S. 22/23). Die KKH hat noch während der Kontrolle die Einrichtung einer selbständigen Beihilfestelle zugesagt und wird die endgültige Lösung mit mir abstimmen.

Ich habe die Kontrolle auch dazu benutzt, zwei Einzelprobleme von grundsätzlicher Bedeutung zu klären, die durch Petenteneingaben an mich herangetragen worden waren.

Für den Vorwurf, die KKH habe mit einem privaten Krankenversicherungsunternehmen, den Austausch von Anschriften der Versicherten ohne deren Wissen vereinbart, ergaben sich keine Anhaltspunkte. Die KKH wies mit einer entsprechenden Dienstanweisung nach, daß Abreden — auch mit weiteren Krankenversicherungsunternehmen — nur unter dem Vorbehalt getroffen worden sind, daß eine Anschriftenweitergabe auf ausdrücklichen Wunsch und mit Einverständnis des jeweiligen Mitglieds erfolgen darf. Die Mitarbeiter der Kasse wurden schriftlich auf die Einhaltung dieser Regelung hingewiesen. Die KKH hat plausibel dargelegt, daß die Weitergabe von Versichertendaten unter diesen Voraussetzungen erforderlich ist, um ihr Beratungsangebot, z. B. zur Sicherstellung des Krankenversicherungsschutzes bei Auslandsreisen zum Ausgleich von Leistungseinschränkungen infolge des Gesundheits-Reformgesetzes, zu ergänzen.

Auch der in einer weiteren Eingabe geäußerte Verdacht, bei der ehrenamtlichen Wahrnehmung der Aufgaben von Außenstellen durch nebenamtlich Tätige könne es aufgrund von Interessenkollisionen zu unzulässigen Offenbarungen von Mitgliederadressen kommen, hat sich bei meiner Kontrolle nicht erhärtet. Vor Ort konnte bei einer der Außenstellen festgestellt werden, daß diese nur sehr begrenzte Einzelaufgaben der Mitgliederbetreuung wahrnehmen, wie z. B. Ausgabe von Krankenscheinscheckheften gegen Verbrauchsnachweis, die Bereithaltung von Informationsmaterial zur gesundheitlichen Aufklärung und über die KKH sowie die Entgegennahme und Weiterleitung von Korrespondenz der Mitglieder an die zuständige Geschäftsstelle. Die Außenstellen halten für diesen Zweck auch nur wenige nicht besonders schützenswerte personenbezogene Daten, wie Name, An-

schrift, Beginn der Mitgliedschaft, Geburtsdatum und ggf. Datum der Ausgabe von Krankenscheinscheckheften vor. Die Außenstellenleiter werden auf das Sozialgeheimnis hingewiesen und in ihrem Vertrag auf dessen Einhaltung verpflichtet. Die KKH betraut mit der Leitung von Außenstellen ausschließlich natürliche Personen und keine Firmen, so daß auch eine persönliche datenschutzrechtliche Verantwortlichkeit begründet wird. Ich habe der KKH empfohlen, bei der Übertragung einer Außenstelle künftig noch stärker auf mögliche Interessenkollisionen, aus denen sich besondere Datenschutzrisiken ergeben könnten, zu achten.

Die KKH hat meine Empfehlungen aufgegriffen und — soweit sich Defizite aufgezeigt haben — deren schnelle Beseitigung zugesichert.

13.3 Werbemaßnahmen einer Krankenkasse

Der im Bereich der gesetzlichen Krankenversicherung wachsende Konkurrenzdruck führt gelegentlich zu fragwürdigen Methoden bei der *Werbung neuer Versicherter*, die auch in das Recht der Betroffenen auf informationelle Selbstbestimmung eingreifen. So hat eine Bezirksgeschäftsstelle einer Ersatzkasse Betriebsprüfungen bei Arbeitgebern dazu genutzt, personenbezogene Daten von Versicherten anderer Krankenkassen unzulässigerweise für Zwecke der eigenen Mitgliederwerbung zu erheben.

Die Ersatzkasse hat den Verstoß eingeräumt und verbindlich zugesagt, dieses Verfahren nicht mehr zu praktizieren.

14 Rentenversicherung

14.1 Rentenreformgesetz 1992

Das auch unter datenschutzrechtlichen Gesichtspunkten bedeutsamste Gesetzgebungsvorhaben im Bereich des Sozialwesens war im Berichtszeitraum die Reform der gesetzlichen Rentenversicherung durch das Rentenreformgesetz 1992 (RRG 1992).

Dieses Gesetz beinhaltet auch die Erhebung und Verarbeitung personenbezogener Daten von Millionen von Bundesbürgern und greift damit in deren verfassungsrechtlich garantiertes Recht auf informationelle Selbstbestimmung ein.

Ich hatte Gelegenheit, meine Überlegungen für einen möglichst guten Datenschutz in der Rentenversicherung gegenüber dem Bundesminister für Arbeit und Sozialordnung und vor mehreren Bundestagsausschüssen (auch in einer öffentlichen Anhörung des Bundestagsausschusses für Arbeit und Sozialordnung) im einzelnen darzulegen. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat hierzu eine Entschließung gefaßt (s. Anlage 4).

Im Ergebnis ist es auf diese Weise gelungen, das RRG 1992 in Einzelregelungen und einem eigenen Abschnitt Datenschutz insgesamt datenschutzrechtlich zufriedenstellend zu gestalten.

Im wesentlichen ging es darum, den Umfang der Datenerhebung und -verarbeitung im Rahmen der gesetzlichen Pflichtversicherung auf das notwendige Maß zu beschränken, den Verwendungszweck sowie Art und Umfang der Daten bereichsspezifisch und präzise zu bestimmen sowie Auskunfts- und Löschungsregelungen festzulegen.

Folgende wichtige datenschutzrechtliche Verbesserungen möchte ich besonders hervorheben:

- Die Aufgaben der Rentenversicherungsträger werden in einem Katalog festgelegt und die dateimäßige Verarbeitung von personenbezogenen Versichertendaten auf die Erfüllung dieser Aufgaben beschränkt (§ 148 Abs. 1).
- Besondere Schutzvorkehrungen sind für Daten getroffen worden, aus denen die Art einer Erkrankung erkennbar ist: Diese Daten dürfen mit anderen Daten in einer gemeinsamen Datei nur gespeichert werden, wenn die Zugriffsrechte der Mitarbeiter strikt aufgabenbezogen abgegrenzt sind (§ 148 Abs. 2).
- Über diese für die Rentenversicherung bereichsspezifisch getroffene Regelung hinaus wird der Grundsatz, daß personenbezogene Daten — unabhängig von der jeweiligen Organisation eines Trägers von Sozialleistungen — nur den Personen zugänglich sein dürfen, die sie für die Erfüllung ihrer Aufgaben benötigen, durch die Ergänzung des § 35 Abs. 1 SGB I mit genereller Wirkung für alle Sozialleistungsträger gesetzlich verankert.
- Ebenfalls generell geregelt wird nunmehr in § 35 Abs. 1 SGB I, daß personenbezogene Leistungs- und Versichertendaten der Beschäftigten von Sozialversicherungsträgern und deren Angehörigen Mitarbeitern mit Personalverwaltungs- und -entscheidungsfunktionen nicht zugänglich sein oder offenbart werden dürfen.
- Die Einrichtung automatisierter Abrufverfahren ist nur zwischen den Trägern der Rentenversicherung und der gesetzlichen Krankenversicherung, der Bundesanstalt für Arbeit und der Deutschen Bundespost, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist, zulässig, sofern dies für diese Stellen zur Erfüllung ihrer Aufgaben erforderlich ist.

  Automatisierte Abrufverfahren auch mit Leistungsträgern außerhalb des Geltungsbereichs des RRG dürfen darüber hinaus nur eingerichtet werden, wenn keine Anhaltspunkte dafür bestehen, daß durch die Übermittlung schutzwürdige Belange der betroffenen Personen beeinträchtigt werden (§ 148 Abs. 3).

  Die Regelungen über automatisierte Abrufverfahren sind lediglich ein genereller Rahmen. Die Einführung solcher Verfahren setzt neben der Einhaltung der datenschutzrechtlichen Bestimmungen über die Einrichtung automatisierter Abrufverfahren voraus, daß die Daten, die online zur Verfügung gestellt werden sollen, nach dem SGB X offenbart werden dürfen. In diesem Zusammenhang gehe ich davon aus, daß die Novelle des BDSG entsprechende gesetzliche Vorgaben für automati-

sierte Abrufverfahren enthalten wird. Ich stimme mit dem Bundestagsausschuß für Arbeit und Soziales darin überein, daß entsprechend diesen Gesetzesvorgaben automatisierte Abrufverfahren nur dann eingerichtet und in Anspruch genommen werden dürfen, wenn dies unter Abwägung der Interessen der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist.

— Die Weitergabe von Daten an den Verband Deutscher Rentenversicherungsträger oder an dessen Datenstelle ist nur strikt aufgabenbezogen oder aufgrund ausdrücklicher gesetzlicher Bestimmung zulässig (§ 148 Abs. 4).

— Versicherungsnummern dürfen von den Trägern der Rentenversicherung nur unter besonderen gesetzlichen Voraussetzungen vergeben werden. Die personenbezogenen Merkmale, die in einer Versicherungsnummer enthalten sein dürfen, sind gesetzlich abschließend festgelegt (§ 147).

— Der Verband Deutscher Rentenversicherungsträger darf nach Versicherungsnummern geordnete Dateien nur bei der Datenstelle führen und nur dann, wenn die Einrichtung der jeweiligen Datei gesetzlich bestimmt ist (§ 146 Abs. 3). Die in diesem Zusammenhang bedeutendste Datei, die Stammsatzdatei aller Personen mit Versicherungsnummern, wird hinsichtlich der Aufgaben, für die sie geführt werden darf, und der personenbezogenen Daten, die in ihr enthalten sein dürfen, näher bestimmt (§ 150).

— Die Einrichtung eines automatisierten Abrufverfahrens für eine Datei der Datenstelle ist nur unter bestimmten Voraussetzungen und nur gegenüber bestimmten Stellen zulässig; der Bundesbeauftragte für den Datenschutz ist von der Einrichtung solcher Verfahren zu unterrichten (§ 150 Abs. 4).

— In § 146 Abs. 4 und 5 wurden bisher umstrittene Fragen nunmehr eindeutig gesetzlich geklärt: Danach unterstehen der VDR und dessen Datenstelle der Aufsicht des Bundesministers für Arbeit und Sozialordnung; sie gelten als öffentliche Stellen des Bundes im Sinne des BDSG und unterliegen damit auch der Kontrolle des Bundesbeauftragten für den Datenschutz.

— Voraussetzungen und Inhalt von Auskünften, die die Deutsche Bundespost den Sozialleistungsträgern und den ihnen gleichgestellten Stellen über die ihr bekannt gewordenen personenbezogenen Daten der Rentenversicherung erteilen darf, werden gesetzlich geregelt (§ 151 Abs. 1 und 2).

— Weitere Konkretisierungen, insbesondere hinsichtlich der Vergabe, Zusammensetzung und Änderung der Versicherungsnummer, Art und Umfang des Datenaustausches, der Führung des Versicherungskontos und der Löschungsfristen bleiben einer Rechtsverordnung vorbehalten (§ 152).

Ich werde die Auswirkungen des Rentenreformgesetzes auf die Praxis der Verarbeitung der personenbezogenen Versichertendaten mit besonderer Aufmerksamkeit verfolgen.

14.2 Rentenversicherung — Einzelfälle

— Der BfA wurde im Rahmen eines Rentenverfahrens bekannt, daß der Antragsteller sich seit längerer Zeit im Strafvollzug befand. Sie fragte daraufhin bei der Justizvollzugsanstalt an, ob gemäß § 50 SGB I *Rentenansprüche* auf diese *übergeleitet* werden sollen. Dies hatte u. a. zur Folge, daß sich die Auszahlung der Rente um mehrere Monate verzögerte. Auf meine Anfrage räumte die BfA ein, daß das beschriebene Tätigwerden von Amts wegen nicht erforderlich war, sondern den Eingang einer schriftlichen Überleitungsanzeige von Seiten des Kostenträgers vorausgesetzt hätte. Ich habe die Anfrage der BfA als Verstoß gegen das Sozialgeheimnis im Sinne des § 35 SGB I gewertet, aber nicht förmlich beanstandet, weil es sich um einen Einzelfall handelte, die BfA den Verstoß eingeräumt und zur Vermeidung künftiger Verstösse eine entsprechende Regelung in die für die Leistungsabteilungen verbindliche Arbeitsanweisung aufgenommen hat.

— Ein Petent beschwerte sich darüber, daß die BfA aufgrund seines Antrags auf Berufs- bzw. Erwerbsunfähigkeitsrente ohne sein vorheriges Wissen einen *Fragebogen an seinen Arbeitgeber* mit der Bitte um Beantwortung und anschließende Rücksendung gerichtet hatte. Der Arbeitgeber erfuhr damit erstmals vom Rentenantrag seines Mitarbeiters. Die BfA wird auf meine Anregung hin den Fragebogen künftig dem Antragsteller selbst mit der Bitte übersenden, ihn zur Ausfüllung an den Arbeitgeber weiterzuleiten. Die Rücksendung an die BfA kann durch den Antragsteller oder auf dessen Wunsch durch den Arbeitgeber erfolgen; darauf wird in dem neu gefaßten Vordruck ausdrücklich hingewiesen.

— Im Rahmen eines Besuches bei den Versorgungsanstalten der Deutschen Bühnen und Kulturorchester in München stellte ich fest, daß die BfA zur Abwicklung etwaiger Rentennachzahlungen mit befreiender Wirkung *Rentenbescheide und Rentenbenachrichtigungen* mit genauer Angabe des Rentenbetrages übersandt hatte, obwohl die Versorgungsanstalten die jeweiligen Nachweise im Regelfall vom Versicherten anfordern und Angaben über die Höhe der von der BfA gewährten Renten nicht benötigen. Die BfA hat auf meine Veranlassung ihre Mitarbeiter in einem Rundschreiben darauf hingewiesen, daß Mitteilungen über eine Rentenbewilligung von Amts wegen künftig zu unterbleiben haben. Entsprechende personenbezogene Daten sind ausschließlich auf Anfrage der Zusatzversorgungskasse unter Angabe der im einzelnen benötigten Informationen weiterzugeben.

15 Unfallversicherung — Bau-Berufsgenossenschaft Wuppertal —

Durch eine Eingabe wurde mir bekannt, daß nicht mehr benötigte EDV-Listen der Bau-Berufsgenossenschaft mit personenbezogenen Daten von einer Mitarbeiterin in wohlmeinender Absicht einem Kindergar-

ten als Malpapier zur Verfügung gestellt worden waren. Diese Listen wurden später in einer Mülltonne gefunden.

Die Bau-Berufsgenossenschaft hat eingeräumt, den Umgang mit Listenausdrucken nicht hinreichend geregelt und überwacht zu haben. Sie hat den Sachverhalt zum Anlaß genommen, ihre Vorkehrungen für die datenschutzgerechte Entsorgung von EDV-Listen und anderen Datenträgern mit personenbezogenen Daten zu überprüfen und geeignete Maßnahmen zu ergreifen, um vergleichbare Vorfälle für die Zukunft auszuschließen.

Ich habe die unzureichenden organisatorischen Regelungen über Aufbewahrung und Vernichtung der EDV-Listen mit personenbezogenen Daten und deren dadurch ermöglichte Weitergabe als unzulässige Offenbarung und Verstoß gegen § 35 SGB I i. V. m. §§ 67 ff. SGB X gemäß § 20 Abs. 1 BDSG beanstandet.

16 Gesundheitswesen

16.1 Krebsregister

Am 5. Dezember 1989 tagte in Bonn die 4. Große Krebskonferenz. Ein wichtiger Punkt der Beratungen war die Erweiterung der Grundlagen für die Krebsepidemiologie, insbesondere durch den Auf- und Ausbau eines flächendeckenden Netzes von regionalen Krebsregistern.

Die Arbeitsgruppe „Epidemiologie" des Deutschen Gesamtprogramms zur Krebsbekämpfung hat in einem Votum vom April 1989 namentlich geführte Krebsregister gefordert. Ebenfalls für eine namentliche Registrierung von Krebserkrankten hat sich das Komitee von Krebsexperten der Europäischen Gemeinschaft in einer Resolution vom 25. Mai 1989 ausgesprochen.

Namentliche Meldungen an Krebsregister sind nur mit Einwilligung der Patienten oder aufgrund von Rechtsvorschriften zulässig. Entsprechende Rechtsvorschriften haben die Länder Hamburg, Saarland und Nordrhein-Westfalen erlassen. Baden-Württemberg hat in einer Feldstudie Krebsregistrierungen mit Hilfe eines „Verschlüsselungsmodells" getestet, das ein Melden von medizinischen Daten durch die behandelnden Ärzte an ein Krebsregister ohne Einwilligung des Patienten zuläßt. Das Modell ermöglicht es, Patientendaten nicht personenbezogen zu melden. Den Daten ist lediglich ein Identifikator beigefügt, der es dem meldenden Arzt ermöglicht, die Daten im Bedarfsfall auf den einzelnen Patienten zurückzuführen.

In meiner Stellungnahme zu den mit einem Krebsregister verbundenen rechtlichen Problemen, die ich im Rahmen der 4. Großen Krebskonferenz am 5. Dezember 1989 in Bonn abgegeben habe (s. Anlage 10), habe ich auf die insbesondere datenschutzrechtlichen Vorteile eines Verschlüsselungsmodells hingewiesen. Wegen der Bedeutung des Themas möchte ich auch an dieser Stelle deutlich machen, daß ich die Bemühungen, auf der Grundlage eines Verschlüsselungsmodelles ein flächendeckendes Netz von regionalen Krebsregistern zu schaffen, unterstütze. Mein Anliegen ist es, die Erfordernisse der wissenschaftlichen Forschung auf diesem wichtigen Gebiet mit dem Recht der Bürger auf Wahrung ihrer Privatsphäre, insbesondere des Arztgeheimnisses, in möglichst hohe Übereinstimmung zu bringen. Ich bin sicher, daß sich dabei ein für beide Seiten gangbarer Weg finden läßt. Nach meiner Auffassung bietet das Verschlüsselungsmodell von den bisher diskutierten Möglichkeiten die beste Grundlage für die notwendigen weiteren Erörterungen.

16.2 KLINAIDS und KLIMACS

Anfang des Berichtsjahres wurden mir die Datenverarbeitungs- programme KLINAIDS (Multizentrische Studie zum Verlauf der HIV-Infektion) und KLIMACS (Klinisch-medizinische Analysen — Computer System) bekannt, die zum Sofortprogramm der Bundesregierung zur AIDS-Bekämpfung gehören.

KLINAIDS soll im Rahmen der Multizentrischen Gemeinschaftsstudie des Bundesministers für Jugend, Familie, Frauen und Gesundheit Daten über Krankenhausaufenthalte von AIDS-Kranken in ausgewählten Zentren mit wissenschaftlicher Forschung erfassen. Das Ziel der Gemeinschaftsstudie ist es, Zusammenhänge von

— Alter und Geschlecht

— Ansteckungswegen

— Vorerkrankungen

— Symptomen bei der Aufnahme

— Art, Dauer und Erfolg der Behandlung

— sozialer Betreuung

— Art und Umfang der ambulanten Betreuung

zu erkennen und zu untersuchen.

Den Kliniken, die sich an dieser Studie beteiligen, wird das Softwarepaket KLINAIDS zur Verfügung gestellt. KLINAIDS kann auf jedem Rechner, der unter dem Betriebssystem MS-DOS läuft, eingesetzt werden.

Unabhängig hiervon fördert der Bundesminister für Arbeit und Sozialordnung die computergestützte Krankendokumentation KLIMACS. KLIMACS soll ebenfalls in Kliniken eingesetzt werden, die AIDS-Patienten betreuen. Es soll deren derzeitige Behandlung und weitere klinische Überwachung sowohl medizinisch als auch organisatorisch verbessern. Hierzu werden die dafür relevanten Daten auf Arbeitsplatzrechnern (stand-alone) verarbeitet. Diese Rechner laufen ebenfalls unter dem Betriebssystem MS-DOS, sie werden im Rahmen der Förderung den Kliniken zur Verfügung gestellt.

Beide Programme — die nach Information der betroffenen Ministerien im Berichtsjahr noch in keiner Klinik mit echten Patientendaten eingesetzt wurden — sollen die Verarbeitung von medizinischen Daten von Patienten unterstützen.

Im Rahmen meiner Beratung habe ich die Ressorts darauf hingewiesen, daß die Patienten einen umfassenden Anspruch auf Aufklärung über den Umfang und den Zweck der automatisierten Datenverarbeitung einschließlich der getroffenen Maßnahmen zur Datensicherung haben und daß ein Sicherheitskonzept für KLINAIDS und KLIMACS entwickelt werden muß, damit den Anforderungen des § 6 Bundesdatenschutzgesetz entsprochen wird. Meine detaillierten Vorschläge hierzu hat der Bundesminister für Arbeit und Sozialordnung auch der Enquete-Kommission AIDS des Deutschen Bundestages bekannt gemacht. Derzeit wird geprüft, ob und mit welchem Sicherheitskonzept KLINAIDS tatsächlich eingesetzt werden soll. Ein Sicherheitskonzept für KLIMACS wird auf der Grundlage meiner Empfehlungen gegenwärtig erarbeitet.

Wenn die Ministerien mich schon in der Planungsphase um Beratung gebeten hätten, hätte sich vermeiden lassen, daß Softwarepakete erstellt, Rechner an Kliniken gegeben und Handbücher für die Nutzer geschrieben wurden, die den Anforderungen des Datenschutzes und der Datensicherheit nicht gerecht wurden. Eine nachträgliche Anpassung von Software und auch die nachträgliche Einführung eines Sicherheitspaketes für einen Rechner ist stets mit einem erheblichen Aufwand verbunden. Ich hoffe, daß ich zukünftig bei Projekten dieser Sensibilität rechtzeitig eingeschaltet werde.

16.3 Bundesgesundheitsamt

Im Rahmen eines Besuches habe ich das Bundesgesundheitsamt unter anderem zu Fragen der Datensicherheit und zur Durchführung der klinischen Prüfung von Arzneimitteln beraten.

— Nach den IT-Richtlinien der Bundesregierung vom 18. August 1988 (GMBl 1988 S. 470ff.) sind Bundesbehörden gehalten, ein Sicherheitskonzept zu erstellen, bevor sie Rechner einsetzen (s. auch 24.1). In einer Behörde wie dem Bundesgesundheitsamt kommt einem solchen Sicherheitskonzept besondere Bedeutung zu, da das Bundesgesundheitsamt an vielen Stellen besonders sensible personenbezogene Daten zum Teil mit Hilfe von Arbeitsplatzrechnern verarbeitet. Die Entscheidung für den Einsatz von Arbeitsplatzrechnern wird — durchaus verständlich — damit begründet, daß man aus Sicherheitsgründen keinen Rechner betreiben möchte, der gleichzeitig anderen Benutzern zur Verfügung steht. Auch diese Entscheidung ist aber nur zu verantworten, wenn vorher ein Sicherheitskonzept festgelegt wird. Ich habe dem Bundesgesundheitsamt insbesondere meine Beratung für die Anwendung eines sinnvollen Sicherheitspaketes für die eingesetzten Arbeitsplatzrechner mit dem Betriebssystem MS-DOS angeboten (s. auch 24.2.4). Zu jedem Sicherheitskonzept gehört aber auch, daß die konkrete Umgebung (Gebäude, Aufbau- und Ablauforganisation), in der die Datenverarbeitung stattfinden soll, berücksichtigt und möglicherweise geändert werden muß. In den Gesprächen mit den Verantwortlichen des Bundesgesundheitsamtes wurde deutlich, daß für die dazu notwendige Systemanalyse nicht das entsprechende Personal zur Verfügung steht. Das Bundesgesundheitsamt hat aber Aufgaben wahrzunehmen, die nur sinnvoll erfüllt werden können, wenn Vertrauen in die Sicherheit seiner automatisierten Datenverarbeitung besteht. Dem Bundesgesundheitsamt sollten deshalb möglichst rasch die erforderlichen Mittel zur Verfügung gestellt werden, damit für besonders schützenswerte Bereiche, wie z. B. das Robert-Koch-Institut, ein professionelles Sicherheitsgutachten erstellt werden kann.

— Der Entwurf einer EG-Richtlinie „Good clinical practice for trials on medicinal products in the European Community" (GCP) sieht u. a. vor, die klinische Prüfung von Arzneimitteln besser kontrollierbar zu machen. Die Beachtung dieser Richtlinie würde Manipulationen während einer solchen klinischen Prüfung erschweren. Das ist im Interesse der Allgemeinheit ein erwünschtes Ergebnis, weil damit Gesundheitsrisiken beim Gebrauch von Arzneimitteln gemindert werden können. Ich habe gegenüber dem Institut für Arzneimittel des Bundesgesundheitsamtes und dem Bundesminister für Jugend, Familie, Frauen und Gesundheit jedoch deutlich gemacht, daß nur vorrangige Interessen der Allgemeinheit rechtfertigen können, das Arztgeheimnis im Rahmen der klinischen Prüfung, wie sie die EG-Richtlinie vorschlägt, unter bestimmten Bedingungen auf der Grundlage einer gesetzlichen Regelung zu durchbrechen. Ich empfehle, in den Siebenten Abschnitt des Arzneimittelgesetzes — Schutz des Menschen bei der klinischen Prüfung — eine entsprechende Regelung mit aufzunehmen. Es sollten Rechtsvorschriften geschaffen werden, die der EG-Richtlinie Rechnung tragen und die von dieser geforderten Maßnahmen erlauben. Nach eingehender Beratung mit Vertretern des Bundesministers für Jugend, Familie, Frauen und Gesundheit wurde davon Abstand genommen, diese Ergänzung in die laufende Novellierung des Arzneimittelgesetzes einzubringen. Mit dem Bundesminister besteht allerdings Einigkeit, daß nach einer Verabschiedung der EG-Richtlinie das Arzneimittelgesetz ergänzt werden muß. Von meinen Überlegungen habe ich auch den Bundesverband der Pharmazeutischen Industrie informiert, der meines Erachtens an einer entsprechenden Änderung des Arneimittelgesetzes schon aus Gründen des Ansehens und damit auch der Konkurrenzfähigkeit der Deutschen Pharmazeutischen Industrie interessiert sein müßte.

16.4 Strahlenschutzregister beim Bundesamt für Strahlenschutz

Bei den Beratungen des Entwurfs eines Gesetzes über die Errichtung eines Bundesamtes für Strahlenschutz (BT-Drucksache 11/4036) wurde deutlich, daß der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit die notwendigen Bestimmungen über die Einrichtung und Nutzung eines zentralen Strahlenschutzregisters nicht auf der Ebene des Gesetzes,

sondern lediglich durch Rechtsverordnung treffen wollte. Entsprechend der zum Recht auf informationelle Selbstbestimmung und zur Wesentlichkeitstheorie ergangenen Verfassungsrechtsprechung bedarf jedoch die zwangsweise Verarbeitung personenbezogener Daten einer normenklaren und verfassungsmäßigen Regelung in einem Gesetz. So ist auch die Einrichtung zentraler Register zur Speicherung personenbezogener Daten ohne Einwilligung des Betroffenen auf anderen Gebieten der Staatstätigkeit jeweils durch eine gesetzliche Regelung erfolgt.

Aus diesem Grunde habe ich bei den Beratungen des Entwurfs dem federführenden Bundestagsausschuß für Umwelt, Naturschutz und Reaktorsicherheit einen Formulierungsvorschlag für eine entsprechende Ergänzung des Atomgesetzes übermittelt. Der Deutsche Bundestag hat diesen Vorschlag voll übernommen, so daß sowohl die Einrichtung und der Betrieb des Strahlenschutzregisters als auch die Überprüfung der beim Umgang mit radioaktiven Stoffen tätigen Personen (s. 19.1) auf einer klaren gesetzlichen Grundlage erfolgen.

Inhaltlich ist neben der Errichtung und Zweckbestimmung eines Dosisregisters bereits im Gesetz eine Pflicht zur Unterrichtung der Betroffenen über die Datenspeicherung vorgesehen. Daneben sind Bedingungen für die Übermittlung von Registerdaten für Zwecke der wissenschaftlichen Forschung aufgenommen worden, mit denen sichergestellt werden soll, daß die schutzwürdigen Belange der Betroffenen gewahrt bleiben. Einzelheiten des Betriebs des Registers und Verfahrensfragen werden auf dieser gesetzlichen Grundlage in der Strahlenschutzregisterverordnung näher geregelt, die die Bundesregierung inzwischen dem Bundesrat zugeleitet hat.

17 Bundeskriminalamt

17.1 Folgerungen aus der Kontrolle der Abteilung Staatsschutz des Bundeskriminalamtes

Meine im Vorjahr durchgeführte Kontrolle bei der Abteilung Staatsschutz (s. 11. TB S. 63) und der dort geführten Datei APIS war auch im Berichtsjahr Gegenstand weiterer Erörterungen mit dem Bundesminister des Innern.

Aufgrund meiner Beanstandung, daß mit den Daten der sogenannten „L-Gruppe" von APIS das äußere Erscheinungsbild und das Verhalten von Personen dargestellt werden kann (s. 11. TB S. 64), ist der Katalog der Merkmale zur Personenbeschreibung reduziert worden. Dies ist aus datenschutzrechtlicher Sicht zu begrüßen. Ich habe aber kritisiert, daß es möglich bleiben soll, „L-Gruppen" auch für „andere Personen" — das sind Personen, die weder verdächtigt noch beschuldigt sind — zu erfassen. Der BMI ist weiterhin der Auffassung, daß bei dieser Personengruppe die „L-Gruppe" zu erfassen sei, wenn die Personalien der erfaßten Person nicht eindeutig feststünden, z. B. bei ausländischen Namen mit unterschiedlichen Schreibweisen. Außerdem sei die Speicherung auch für Zwecke der Observation und der polizeilichen Beobachtung erforderlich, um die Identifizierung zu ermöglichen.

Die Speicherung von Daten der „L-Gruppe" bei „anderen Personen" halte ich im Falle von unklaren Personalien für weniger problematisch. Gegen die Speicherung zum Zwecke der Observation oder der polizeilichen Beobachtung habe ich jedoch erhebliche Bedenken, weil es sich dabei um einen zusätzlichen Eingriff gegenüber einer namentlich bereits feststehenden nicht verdächtigten Person handelt. Der BMI prüft derzeit, in wie vielen Fällen „L-Gruppen" zu namentlich feststehenden „anderen Personen" in APIS erfaßt und ob diese für die Belange des Staatsschutzes weiterhin erforderlich sind. Das Ergebnis dieser Prüfung soll in die weitere Erörterung einfließen.

Meine Anregung, „andere Straftaten" nur dann zu erfassen, wenn sie von der Schwere her mit den benannten Staatsschutzdelikten vergleichbar sind, wenn sie überörtliche Bedeutung haben, wenn ihr verfassungsfeindlicher Charakter eindeutig festgestellt oder aufgrund klarer Indizien vermutet werden kann und wenn beim Täter Wiederholungsgefahr besteht, ist der BMI auch nach weiteren Erörterungen nicht gefolgt. Es handelt sich hierbei um Straftaten des allgemeinen Strafrechts, die in APIS erfaßt werden, wenn zu vermuten ist, daß der Täter extremistische Ziele verfolgt, z. B. Sachbeschädigung in Form von Farbschmierereien (s. 11. TB S. 63). Nach Auffassung des BMI wäre es nicht mehr möglich, sog. extremistische Karrieren zu erfassen, wenn meiner Anregung gefolgt würde. Er weist weiter darauf hin, daß grundsätzlich nicht jede Straftat mit politischer Motivation erfaßt wird; Erfassungskriterium sei vielmehr die verfassungsfeindliche Zielrichtung des Straftäters. Im Hinblick auf die bei meiner Prüfung getroffene Feststellung, daß 75 % aller in APIS gespeicherten Straftaten eher leichterer Art waren, halte ich an meiner vorstehend geschilderten Auffassung fest und habe deshalb gefordert, die Errichtungsanordnung für APIS erheblich zu konkretisieren. Im Anschluß an meine Prüfung hat eine Fachkommission aus Bund und Ländern neue Kriterien für die Definition des Begriffs „verfassungsfeindliche Zielsetzung" entwickelt. Der BMI hat angeboten, diese Kriterien weiter einzugrenzen und die mit APIS arbeitenden Polizeibeamten entsprechend zu schulen. Das Ergebnis der Beratungen der Kommission Staatsschutz soll weiter mit mir erörtert werden. Ich habe meine Bereitschaft zur weiteren Beratung erklärt. Auch wenn meine Anregungen nur teilweise berücksichtigt werden, könnte dies zu einer erheblichen Reduzierung der Erfassung „anderer Straftaten" führen.

Einigkeit wurde mit dem BMI dahingehend erzielt, daß auch die sog. „klassischen" Staatsschutzdelikte nicht schematisch erfaßt werden dürfen, wie ich dies insbesondere bei der Speicherung von Straftaten nach § 86 a StGB in der Form des Verwendens von nationalsozialistischen Symbolen festgestellt habe (s. 11. TB S. 64). Auch hier soll die Kommission Staatsschutz zusätzliche Erfassungskriterien — wie bei den „anderen Straftaten" — erarbeiten.

17.2 Kontrolle beim Referat TB 22 des Bundeskriminalamtes

Das Referat TB 22, das die Datenerfassung und die Datenpflege für den Aktennachweis des BKA durchführt, hat für den Datenschutz im BKA zentrale Bedeutung. Dort gehen täglich etwa 2 000 Meldungen ein, die zum Teil zu einer erstmaligen Einspeicherung in das Polizeiliche Informationssystem führen (ca. 35 %) zum überwiegenden Teil aber Veränderungen im Datenbestand auslösen. Daneben werden dort monatlich rund 20 000 Datensätze gelöscht.

Die Arbeit des Referates war erstmals im Jahre 1985 Gegenstand einer Datenschutzkontrolle, die zu beanstandungen und zu zahlreichen Empfehlungen geführt hatte. Mit der 1989 begonnenen Kontrolle sollte geklärt werden, ob diesen Empfehlungen entsprochen wurde und die Datenverarbeitung jetzt keinen Anlaß zu Beanstandungen mehr bietet.

Die Kontrolle ist außerordentlich zeitaufwendig, weil nur durch die Prüfung der einer Speicherung zugrundeliegenden Meldungen und sonstigen Unterlagen festgestellt werden kann, ob die Verarbeitungskriterien insbesondere in bezug auf den Grund und die vorgesehene Dauer einer Speicherung eingehalten worden sind. Um aussagekräftige Ergebnisse zu erreichen, haben meine Mitarbeiter mehrere unterschiedlich geschnittene Stichproben mit insgesamt über 200 Fällen gezogen.

Infolge der angespannten Personalsituation konnte die im Juli begonnene Kontrolle im Berichtsjahr noch nicht zu Ende geführt werden; dies soll nun im Jahre 1990 geschehen.

17.3 Datenabfrage zur Besucherkontrolle

Im Jahre 1987 habe ich das vom Bundeskriminalamt praktizierte Verfahren der Besucherkontrolle beanstandet (s. 10. TB S. 79). Das Bundeskriminalamt überprüft Besucher, die nicht persönlich bekannt sind, durch Abfrage seiner automatisierten Dateien. Findet sich eine nachteilige polizeiliche Information, so wird der Besucher abgewiesen. Dies hatte beispielsweise dazu geführt, daß ein Journalist einen wissenschaftlichen Mitarbeiter des Amtes nicht an dessen Arbeitsplatz aufsuchen konnte, weil ein Landeskriminalamt Daten eingegeben hatte, die auf polizeiliche Ermittlung wegen des Verdachts einer Beleidigung mit politischem Bezug hinwiesen. Tatsächlich war der Journalist von einem Restaurantbesitzer wegen Beleidigung angezeigt worden, nachdem er dessen Leistungen in einer alternativen Zeitschrift kritisiert hatte; nur wegen des Charakters der Zeitschrift war er in den Verdacht eines Staatsschutzdelikts geraten. Das Bundeskriminalamt hat mir kürzlich mitgeteilt, es habe die Zugangskontrolle dahingehend geregelt, daß amtsfremde Personen bzw. Personen ohne Dienstausweise aufgefordert werden, ihr Einverständnis für eine „personenbezogene Überprüfung" zu erklären. Werde das Einverständnis nicht erteilt, so würden die Besucher in einem Raum vor dem Sicherheitsbereich betreut.

Diese Regelung bleibt datenschutzrechtlich unbefriedigend. Die geforderte Einverständniserklärung geht zu weit und ist inhaltlich unklar. Ich hatte vorgeschlagen, die Abfrage von personenbezogenen Daten auf die Ermittlung sicherheitsrelevanter Umstände zu beschränken, die Sicherheitsrelevanz der Erkenntnisse im Einzelfall zu bewerten und sicherzustellen, daß Dritte, insbesondere der besuchte Bedienstete, über Erkenntnisse nur im erforderlichen Umfang unterrichtet werden. Ich habe das Bundeskriminalamt um Erläuterung gebeten, warum keinem dieser Punkte gefolgt werden soll. Die Antwort des BKA hat die Fragen nicht geklärt. Ich muß darauf hinweisen, daß sich der oben beschriebene Fall nach der neuen Regelung genauso wiederholen könnte.

17.4 Fortentwicklung der Datenverarbeitung beim Bundeskriminalamt

Das Bundeskriminalamt betreibt zur Unterstützung von Ermittlungsverfahren derzeit 42 SPUDOK-Dateien in den unterschiedlichsten Anwendungsgebieten. Neben Anwendungen in den Deliktsbereichen Terrorismus, Bandenkriminalität und Kapitalverbrechen werden jetzt zunehmend auch in Fällen der allgemeinen Kriminalität SPUDOK-Dateien eingesetzt. Allein im Berichtsjahr wurden mir siebzehn neue SPUDOK-Anwendungen gemeldet. Über die mit dem Verfahren SPUDOK möglichen Recherchen und die damit verbundenen datenschutzrechtlichen Fragen habe ich berichtet (7. TB S. 66; 8. TB S. 45). Problematisch ist insbesondere die Speicherung von Daten „anderer Personen", d. h. Personen, die weder Beschuldigte noch Verdächtigte sind.

Meine Anregung, Daten „anderer Personen" nur im Rahmen der Zwecke zu verwenden, denen die SPUDOK dient (s. 11. TB S. 63) hat der Bundesminister des Innern inzwischen aufgegriffen. Ich gehe davon aus, daß nunmehr eine Nutzung für andere Zwecke, insbesondere in der Form der Übermittlung an Dritte, ausgeschlossen ist.

Auf der anderen Seite hat sich für diesen Personenkreis jetzt eine erhebliche Verschlechterung ergeben, weil entgegen der bisherigen Praxis die Daten nach einjähriger Speicherfrist nicht mehr gelöscht werden, sondern — wie die Daten von Beschuldigten und Verdächtigten — erst dann, wenn das zugrunde liegende Strafverfahren rechtskräftig abgeschlossen ist. Nach Abschluß der Ermittlungen werden die Daten lediglich gesperrt. Eine Benachrichtigung der Betroffenen, die durch Ziffer 4.5 der Dateienrichtlinien grundsätzlich vorgeschrieben ist, unterläßt das BKA durchgängig mit der stereotypen, bereits in den Errichtungsanordnungen niedergelegten Begründung, daß sonst die Ermittlungen gefährdet werden könnten. Die bei einigen SPUDOK-Anwendungen vorgesehene Möglichkeit der Auskunftserteilung auf Antrag der „anderen Person" mildert diese Verschlechterung kaum, denn die Betroffenen, zu denen Daten oft nur erfaßt sind, weil ihr Name in einer Kartei oder einem Notizbuch gefunden wurde, ahnen in aller Regel nichts von ihrer datenmäßigen Erfassung (s. auch 11. TB S. 62f.).

Die drei ältesten mir gemeldeten SPUDOK-Dateien, in der Daten „anderer Personen" gespeichert und bis heute nicht gelöscht sind, wurden 1983 eingerichtet. Hier werden die Daten von „anderen Personen" länger gespeichert als die Daten von Beschuldigten, die im Verdacht von Straftaten geringer Bedeutung (z. B. Diebstahl) stehen, wo die Speicherfrist drei Jahre beträgt. Ein Abschluß der Ermittlungen bei den genannten drei Anwendungen, geschweige der rechtskräftige Abschluß der Strafverfahren, ist noch nicht abzusehen.

Auch der Einsatz von APC im BKA nimmt zu. Immer mehr Datensammlungen, die bisher vom kriminalpolizeilichen Sachbearbeiter als Handkartei geführt worden sind, werden auf APC übertragen. Das BKA hat mir inzwischen siebzehn Anwendungen, die personenbezogene Daten enthalten und noch aktuell auf APC betrieben werden, zum besonderen Dateien-Register gemeldet. Allein acht APC-Anwendungen werden geführt, um Hinweise zu konkreten Ermittlungsverfahren auszuwerten. Zwar ist der Zugriff bei diesen Anwendungen auf das zuständige Referat beschränkt, durch die Verwendung eines Datenbanksystems, das die Recherche und Verknüpfung jedes Datenfeldes ermöglicht, wird jedoch eine neue Qualität der Datenverarbeitung erreicht. Die vom BKA angekündigte Dienstanweisung für den Einsatz und den Betrieb von APC (s. 11. TB S. 63) ist noch nicht erlassen worden. Im Hinblick auf die mit dem Einsatz von APC verbundenen Datensicherheitsprobleme, über die ich bereits mehrfach berichtet habe, (u. a. 8. TB S. 56f.) und der Zahl der schon jetzt betriebenen APC-Anwendungen halte ich eine solche Dienstanweisung für dringend geboten. In dieser Dienstanweisung sollte auch geregelt werden, wann SPUDOK-Dateien geschaffen und wann APC-Anwendungen betrieben werden dürfen. Bisher kann ich keine klare Abrenzung erkennen.

APC-Anwendungen dienen auch als Hilfe zur Verdachtsverdichtung. Erfaßt werden z. B. Hinweise über Personengruppen, bei denen die Vermutung besteht, daß sie im Bereich der organisierten Kriminalität tätig sein könnten, ohne daß bisher ein Ermittlungsverfahren eingeleitet ist. Die APC-Anwendung soll vielmehr den Verdacht so weit erhärten, daß ein Verfahren eingeleitet werden kann. Es handelt sich also um eine Speicherung und Verarbeitung von Erkenntnissen im Vorfeld eines Straftatverdachts im Sinne von § 160 Abs. 1 StPO, der die Eröffnung eines Ermittlungsverfahrens rechtfertigt. Eine automatisierte Verarbeitung personenbezogener Daten im Vorfeld eines Ermittlungsverfahrens erscheint rechtlich bedenklich. Grundsätzlich sind Maßnahmen der Strafverfolgung, die in die Rechte von Einzelpersonen eingreifen, an einen Straftatverdacht gebunden, der die Eröffnung eines Ermittlungsverfahrens rechtfertigt. Es ist Aufgabe des Gesetzgebers zu entscheiden, unter welchen Voraussetzungen, in welchem Umfang und unter Beachtung welcher verfahrensmäßiger Grundrechtssicherungen eine Vorverlagerung von Maßnahmen der Strafverfolgung zulässig sein soll. Ich habe den Bundesminister des Innern auf diese Problematik hingewiesen.

Für problematisch halte ich auch die Speicherung von Daten über sog. „andere Personen" in Dateien, die auf APC geführt werden. Wie bei den SPUDOK-Anwendungen werden diese Personen nach Ablauf eines Jahres entgegen den Dateien-Richtlinien nicht über die Speicherung unterrichtet. Auch hier können die Fristen bis zur Löschung der Daten länger sein als sonst bei den Daten Beschuldigter.

Die Vielzahl der beim BKA betriebenen DV-Anwendungen erschwert mir die Ausübung der datenschutzrechtlichen Kontrolle, wenn sich Betroffene an mich gewandt haben. Bisher ist es erst in einigen wenigen Fällen vorgekommen, daß das BKA auf meine Anfrage nicht alle in Betracht kommenden SPUDOK-Dateien abgefragt hat, mit der Folge, daß den Betroffenen unvollständige, d. h. fehlerhafte Auskünfte erteilt wurden, die dann später berichtigt werden mußten. Diese Gefahr vergrößert sich zwangsläufig mit der Zahl der Dateien. Gleichzeitig verlängert sich die Zeit, die das BKA benötigt, um meine Fragen nach vorhandenen Speicherungen personenbezogener Daten korrekt beantworten zu können. Das BKA muß die erforderlichen organisatorischen Vorkehrungen treffen, um solche Fehler und Schwierigkeiten zu vermeiden. Es gehört zu den gesetzlichen Aufgaben des BKA, auch für die Zukunft sicherzustellen, daß Betroffenen, die sich direkt oder über mich nach der Speicherung ihrer Daten erkundigen, in zumutbarer Frist eine umfassende und korrekte Auskunft erteilt werden kann. Ich mußte dem BKA mitteilen, daß ich eine Bearbeitungsdauer von annähernd drei Monaten nicht akzeptieren kann. Die aufgezeigten Fehler und Schwierigkeiten sollten aber auch Anlaß sein, die Notwendigkeit der einen oder anderen Datei kritisch zu überprüfen. Gemäß einer eigenen Veröffentlichung des BKA (HAUSLESE vom 15. Oktober 1989) haben nach der Errichtung von Dateien angestellte Effizienzprüfungen ergeben, „daß einige Dateien nicht notwendig waren oder mit bereits bestehenden Lösungen hätten gekoppelt werden können". Ich rege dringend an, derartige Effizienzüberlegungen regelmäßig vor der Einrichtung neuer Dateien durchzuführen.

17.5 Zugriff auf die Falldatei Rauschgift

Ich habe darüber berichtet (s. 9. TB S. 58), daß in der Falldatei Rauschgift (abweichend vom KAN-Konzept) alle Straftaten zentral gespeichert werden, auch wenn es sich nur um Kleinkriminalität im Zusammenhang mit Rauschgift handelt. Meine Forderung, Hinweise auf diese Speicherungen nur bei Zugriffen von Dienststellen auszugeben, die für die Bekämpfung der Rauschgiftkriminalität zuständig sind, hatte der Bundesminister des Innern bisher abgelehnt. Er hat mir nunmehr mitgeteilt, daß diese Hinweise grundsätzlich nur noch dann ausgegeben werden, wenn es sich um Fälle handelt, die im Kriminalaktennachweis zu erfassen sind. Damit ist meiner Forderung entsprochen.

18 Zollkriminalinstitut

18.1 Benachrichtigung anderer Dienststellen von zollrechtlichen Ausschreibungen

Auf meine Forderung hin (vgl. 7. TB S. 72) sind die Datenbestände der zollrechtlichen Überwachung im INPOL — Personenfahndungsbestand — von den anderen Datenbeständen der polizeilichen Beobachtung getrennt worden. Nach der inzwischen durchgeführten Änderung der Polizeidienstvorschrift 384.2 ist ein Informationsaustausch zwischen Zoll und Polizei im Inland bei Ausschreibungen von Personen zur zollrechtlichen Überwachung ausgeschlossen, weil eine Übermittlung von personenbezogenen Daten dieser Personen an Polizeidienststellen im Inland grundsätzlich nicht mit dem Steuergeheimnis vereinbar ist. Eine Unterrichtung der Polizei halte ich dann für zulässig, wenn bei zollrechtlichen Grenzkontrollen wegen einer zollrechtlichen Überwachungsmaßnahme Betäubungsmittel aufgefunden worden sind. Für diesen Fall sieht die PDV 386.1 auch eine Rauschgiftsofortmeldung vor.

Wie ich feststellen konnte, hat das Zollkriminalinstitut entgegen diesem Übermittlungsverbot bei der Ausschreibung einer Person zur zollrechtlichen Überwachung das BKA hierüber unterrichtet und damit gegen das Steuergeheimnis verstoßen. Aufgrund eines Hinweises, dessen Aussagekraft nicht weiter nachgeprüft werden konnte, vermutete man, daß die Person zu einem bestimmten Zeitpunkt Betäubungsmittel ins Ausland schmuggeln würde. Bei den Kontrollen, denen sie unterzogen worden ist, wurden Betäubungsmittel indessen nicht gefunden. Die Ausschreibung wurde daraufhin gelöscht. Ich habe die Übermittlung der personenbezogenen Daten durch das Zollkriminalinstitut an das Bundeskriminalamt beanstandet. Der Bundesminister der Finanzen hat — erst nach einer längeren Auseinandersetzung über die datenschutzrechtliche Beurteilung dieses Falles — das Zollkriminalinstitut angewiesen, das Übermittlungsverbot künftig zu beachten. Zur Vermeidung von Zweifeln weise ich darauf hin, daß ich selbstverständlich keine Bedenken gegen eine Übermittlung von Daten der zollrechtlichen Überwachung an die mit der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs betrauten Polizeidienststellen habe, soweit diesen auch zollrechtliche Aufgaben und Befugnisse zugewiesen sind, wie z. B. nach § 67 des BGS-Gesetzes.

18.2 Bereithaltung von Daten der zollrechtlichen Überwachung zum Abruf beim innerdeutschen Flugverkehr

Der Datenbestand der „Zollrechtlichen Überwachung" dient gemäß der einschlägigen PDV 384.2 der Überwachung nach zollrechtlichen Bestimmungen durch Zolldienststellen. Im Rahmen der Prüfung einer Eingabe habe ich festgestellt, daß die Berliner Polizei die Daten der „Zollrechtlichen Überwachung" auch bei der Kontrolle von Flugreisen von Berlin (West) in das Bundesgebiet abruft und im Trefferfalle Meldungen an das ausschreibende Zollkriminalinstitut abgibt. Ich habe das Bereithalten dieser Daten durch das Zollkriminalinstitut für diesen Zweck wegen Verstoßes gegen § 3 BDSG in Verbindung mit § 2 Abs. 2 Nr. 2 BDSG und gegen das Steuergeheimnis nach § 30 Abgabenordnung beanstandet.

Der Bundesminister der Finanzen ist der Auffassung, daß es sich auf dem Hintergrund des besonderen Status von Berlin bei den genannten Kontrollen der Berliner Polizei um Grenzkontrollen handele. Die Berliner Polizei erfülle insoweit gleiche Aufgaben wie der Bundesgrenzschutz. Sie dürfe auf den Bestand der „Zollrechtlichen Überwachung" auch bei der Grenzabfertigung außerhalb des internationalen Bereichs zugreifen. Der Bundesminister der Finanzen beruft sich im übrigen auf die Order der Berliner Kommandantur BK/O (70) 3 vom 29. Juni 1970 zur „Kontrolle von Reisedokumenten auf den Berliner Flughäfen". Diese alliierte Order verpflichtet die Berliner Polizei, bei Personen, die Berlin auf dem Luftwege verlassen, „eine Kontrolle der Reisedokumente" durchzuführen.

Die Argumentation des BMF ist nicht schlüssig. Es kann dahingestellt bleiben, ob der Flugverkehr zwischen Berlin und dem übrigen Bundesgebiet grenzüberschreitender Verkehr im Sinne des Grenzpolizeirechts (etwa des BGS-Gesetzes) ist. Auf keinen Fall wird bei solchen Flügen aber eine Zollgrenze überquert. Dem entspricht es, daß dabei die Reisenden niemals befragt werden, ob sie etwas zu verzollen haben. Eine zollrechtliche Kontrolle findet deshalb sowohl rechtlich als auch tatsächlich bei Flügen von Berlin in das übrige Bundesgebiet ebensowenig statt wie bei Reisebewegungen zwischen anderen Flughäfen der Bundesrepublik Deutschland. Auch dort werden Daten der „Zollrechtlichen Überwachung" bei Inlandsflügen nicht abgerufen. Es ist nicht einzusehen, warum bei Flügen von Berlin in das übrige Bundesgebiet etwas anderes gelten soll.

Auch die vom BMF erwähnte Order der Berliner Kommandantur rechtfertigt Zollkontrollen bei Flügen von Berlin in das übrige Bundesgebiet nicht. Die Order enthält nach Wortlaut und Regelungszweck keinerlei Elemente, aus denen eine Verpflichtung zur Durchführung von Zollkontrollen entnommen werden kann. Noch weniger enthält sie Anhaltspunkte dafür, daß die Alliierten einen Abruf von Daten der „Zollrechtlichen Überwachung" bei der Kontrolle des Personenverkehrs von Berlin in das Bundesgebiet wünschen. Ich habe den Bundesminister der Finanzen auf die Bedenken hingewiesen, ob den Alliierten überhaupt eine Befugnis zukommt, einen Zugriff auf eine vom Bund im Bundesgebiet betriebene Datei anzuordnen. Der Bundesminister der Finanzen sieht diese Befugnis gegeben. Er verweist hierzu auf die Verpflichtung der Bundesrepublik nach Artikel 6 Abs. 2 des Deutschlandvertrages, mit den Drei Mächten zusammenzuwirken, um es ihnen zu erleichtern, ihren Verantwortlichkeiten in bezug auf Berlin zu genügen. Auch dieses Argument erscheint mir unschlüssig, da der Bundesminister der Finanzen weder vorträgt, daß die Drei Mächte die Bundesrepublik um eine Mitwirkung in der Form der Bereitstellung bestimmter Dateien zum Zugriff durch die Berliner Polizeibehörden ersucht haben, noch ersichtlich ist, wie diese Maßnahme es den

Drei Mächten erleichtern könnte, ihren Verantwortlichkeiten in bezug auf Berlin zu genügen.

Der Bundesminister der Finanzen hatte schon vor meiner Beanstandung darauf hingewiesen, daß nach Artikel 3 Abs. 2 des Gesetzes der Alliierten Kommandatura Nr. 7 „Gerichtsbarkeit auf den vorbehaltenen Gebieten" in der Fassung des Änderungsgesetzes Nr. 17 vom 27. August 1951 (GVBl. S. 639), die mit der Sache befaßten Berliner Behörden das Verfahren aussetzen und die Frage an den zuständigen Sektorkommandanten dann zu überweisen haben, wenn über das Bestehen, den Inhalt, die Rechtsgültigkeit oder den Zweck einer Anordnung der Besatzungsbehörden oder der Besatzungsstreitkräfte zu entscheiden ist, und daß er — sollte ich meine Bedenken aufrechterhalten — prüfen werde, ob nicht entsprechend dieser Vorschrift zu verfahren sei. Ich habe demgegenüber deutlich gemacht, daß meine Beanstandung keine Entscheidung dieses Inhalts erfordert, so daß für eine Vorlage an die Sektorkommandanten kein Anlaß besteht. Statt dessen habe ich daran erinnert, daß ich schon im Jahre 1988 eine Korrektur der Zugriffsbefugnis der Berliner Polizei für geboten erklärt habe. Gleichwohl hat der Bundesminister der Finanzen das Auswärtige Amt, das Bundeskanzleramt, den Bundesminister der Justiz und den Bundesminister für innerdeutsche Beziehungen um Stellungnahme zu meiner Beanstandung gebeten, „ggf. mit dem Ziel, ein Verfahren gemäß Artikel 3 Abs. 2 des Gesetzes der Alliierten Kommandatura Nr. 7" einzuleiten. Ich halte dieses Verfahren nach wie vor nicht für angebracht. Dieses Verfahren kann im übrigen leicht den Eindruck erwecken, deutsche Stellen seien bemüht, sich eine Auslegung einer Alliierten Weisung zu besorgen, die weiterhin als scheinbare Rechtfertigung für eine dem deutschen Recht widersprechende Praxis bei der Bereitstellung von Daten der Zollrechtlichen Überwachung für die Kontrolle von Inlandsflügen durch die Berliner Polizei dienen soll.

19 Bundesamt für Verfassungsschutz

19.1 Sicherheitsüberprüfungen

Die neuen Sicherheitsrichtlinien, die die Sicherheitsüberprüfungsrichtlinien für Bundesbedienstete aus dem Jahre 1971 ablösen, haben in vielen Bereichen Verbesserungen gebracht. Insbesondere konnte dem angestrebten Zweck „mehr Qualität als Quantität" Rechnung getragen werden. In der Vergangenheit hat es sich immer als schwierig erwiesen, sicherheitsempfindliche Bereiche zu definieren und abzugrenzen. Aufgrund der neuen Richtlinien werden diese Bereiche von den jeweils zuständigen Geheimschutzbeauftragten und dem Bundesminister des Innern überprüft. So konnte beispielsweise im Bereich der Flugsicherung die Zahl der zu überprüfenden Personen um über 3 000 gesenkt werden, weil deren Tätigkeiten als nicht sicherheitsempfindlich im Sinne des § 3 Abs. 2 Nr. 4 der Sicherheitsrichtlinien eingestuft wurden. Zum Jahresende hat das Kabinett eine Änderung der Sicherheitsrichtlinien beschlossen, mit der die Anzahl der Sicherheitsüberprüfungen noch einmal um 80 % auf dann ca. 30 000 verringert werden soll. Nur noch „eigentliche Geheimnisträger" sollen überprüft werden, jedoch nicht mehr ganze Dienststellen.

Nach wie vor erfolgen allerdings die Sicherheitsüberprüfungen und die damit verbundenen Eingriffe in die informationelle Selbstbestimmung der Beteiligten ohne eine ausreichende gesetzliche Grundlage (s. 11. TB S. 60f.). Das seit langem angekündigte Geheimschutzgesetz wird, soweit absehbar, in der laufenden Legislaturperiode nicht mehr zustande kommen. Bei Anfragen von Bürgern, die wissen wollen, ob sie Auskunftspersonen benennen und über bestimmte Auslandsreisen und -verbindungen Auskunft geben müssen, habe ich bisher auf die Rechtsprechung des Bundesverfassungsgerichts verwiesen, wonach eine behördliche Maßnahme unter bestimmten Voraussetzungen im unerläßlichen Umfang weiter geführt werden darf, auch wenn keine ausreichende gesetzliche Grundlage besteht („Übergangs-Bonus"). Sechs Jahre nach Verkündung des Volkszählungsurteils kann ich bei den Fragestellern allerdings kaum noch mit Verständnis für eine solche Argumentation rechnen. Es ist absehbar, daß es bei der Praxis der Sicherheitsüberprüfungen erneut zu Schwierigkeiten kommen wird.

Praktische Probleme gibt es bei der Trennung von Geheimschutz und Personalverwaltung. Ein Mitarbeiter der Deutschen Bundespost beschwerte sich bei mir, nachdem ihm die Personalstelle Informationen aus dem Bundeszentralregister vorgehalten hatte. Das Bundeszentralregister hatte diese Information nach § 41 Abs. 1 Nr. 3 BZRG dem Bundesamt für Verfassungsschutz für die ihm übertragenen Sicherheitsaufgaben übermittelt (unbeschränkte Auskunft). Von dort war sie im Zusammenhang mit einer Sicherheitsüberprüfung an den Sicherheitsbeauftragten der Dienststelle der Bundespost gelangt. Nach § 41 Abs. 4 BZRG wird dem Bundesamt für Verfassungsschutz die Auskunft nur auf ausdrückliches Ersuchen und für den bestimmten Zweck übermittelt. Eine Verwendung im Rahmen der Personalverwaltung ist danach ausgeschlossen. Dementsprechend verlangt auch § 16 Abs. 1 der Sicherheitsrichtlinien ausdrücklich eine Trennung zwischen Sicherheitsakten und Personalakten. Der Bundesminister für Post und Telekommunikation erklärte den Vorgang damit, daß der Geheimschutzbeauftragte dem betroffenen Mitarbeiter der Personalverwaltung unterstellt sei und ein gegenseitiges Vertretungsverhältnis bestehe. Dies ändert allerdings nichts an der Zweckbindung der aus dem Bundeszentralregister stammenden Informationen. Nachdem ich eine Beanstandung ausgesprochen hatte, hat der Bundesminister für Post und Telekommunikation seine Mittelbehörden auf die gebotene strikte Trennung von Personalverwaltung und Sicherheitsüberprüfungsverfahren noch einmal besonders hingewiesen.

Die Überprüfung des Personals von Kernkraftwerken hat im Berichtsjahr eine gesetzliche Regelung erfahren (§ 12d Atomgesetz in der Fassung des Gesetzes über die Errichtung eines Bundesamtes für Strahlenschutz vom 9. Oktober 1989, BGBl I S. 1830ff.). Dieses als Zuverlässigkeitsprüfung bezeichnete Verfahren ist zwar der Sicherheitsüberprüfung in manchem ähn-

lich, unterscheidet sich aber doch in wichtigen Punkten von dieser. Zur Unterstützung der parlamentarischen Beratungen habe ich — neben dem zuständigen Ministerium — Hinweise gegeben, die weitgehend übernommen wurden. Von grundlegender Bedeutung ist die nunmehr gesicherte Transparenz des Verfahrens für den Betroffenen: Schon dessen Einleitung setzt sein Einverständnis voraus; wenn Bedenken gegen die Zuverlässigkeit auftauchen, ist der Betroffene dazu zu hören. Eine wie immer geartete heimliche Überprüfung und berufliche Nachteile, denen der Betroffene wehrlos ausgesetzt ist, sollen damit vermieden werden. Diese Grundesätze müssen auch bei vergleichbaren Überprüfungsverfahren, etwa bezüglich des im Luftverkehr tätigen Personals, Beachtung finden.

19.2 Verbunddatei ADOS

Seit Anfang 1989 betreibt das Bundesamt für Verfassungsschutz gemeinsam mit den Landesämtern für Verfassungsschutz die Verbunddatei ADOS (Adressen und Objekte Ost). Die Datei dient der Speicherung der Wohnanschriften und der Beschäftigungsstellen von Aus- und Übersiedlern aus den osteuropäischen Ländern und der DDR aus den Jahren vor deren Übertritt in die Bundesrepublik Deutschland. Namen und aktuelle Anschriften der Betroffenen werden nicht gespeichert. Die Namen und die Anschrift des ersten in der Bundesrepublik genommenen Wohnsitzes sind jedoch mit Hilfe der Unterlagen der bundesdeutschen Aufnahmestellen festzustellen, deren Aktenzeichen in ADOS festgehalten werden. Die Datei dient im Rahmen der Spionageabwehr dazu, im Bedarfsfall Auskunftspersonen zu gewinnen, die etwas über die Bewohner eines bestimmten Hauses oder die Verhältnisse an einer Arbeitsstätte zu einem bestimmten Zeitpunkt sagen können. Dadurch soll es möglich sein, von gegnerischen Nachrichtendiensten eingeschleuste Agenten zu erkennen oder einen entsprechenden Verdacht zu entkräften.

Als das Projekt Anfang 1987 vorgestellt worden war, wurden mit Rücksicht auf die Bedeutung der Spionageabwehr und den relativierten Personenbezug einerseits sowie im Hinblick auf die zu erwartende Schaffung einer bereichsspezifischen, die Datei ADOS abdeckende Rechtsgrundlage für die Datenverarbeitung der Verfassungsschutzbehörden andererseits keine grundsätzlichen Bedenken gegen das Projekt der Verfassungsschutzbehörden erhoben.

Vor dem Innenausschuß des Deutschen Bundestages habe ich dargelegt, daß eine grundsätzliche Neubewertung des Verfahrens erfolgen sollte:

a) Die Anzahl der Aus- und Übersiedler liegt heute um ein Mehrfaches höher als von den Behörden damals vorausgesehen. An die geplante Erfassung aller Personen über achtzehn Jahren ist nicht mehr zu denken. Auswahlkriterien wurden nicht festgelegt. Dies erscheint auch sehr schwierig, wenn das bisher für die datenschutzrechtliche Bewertung maßgebliche Konzept, nach dem die Erfassung keinerlei diskriminierenden oder sonst belastenden Charakter haben darf, nicht verlassen werden soll.

b) Das ursprünglich als hochrangige Verschlußsache eingestufte Verfahren ist mittlerweile auch amtlicherseits in vielen Einzelheiten öffentlich bekanntgegeben worden. Sein Wert für die Sicherheit der Bundesrepublik Deutschland ist dadurch entsprechend geringer.

c) Für die rechtliche Beurteilung ist bedeutsam, daß der von der Bundesregierung vorgelegte Entwurf eines Bundesverfassungsschutzgesetzes keine spezielle Ermächtigung zur Erhebung und Verarbeitung von Daten nicht verdächtiger Personen vorsieht. Eine Speicherung der Daten einer Vielzahl von Personen, die sich von der Bevölkerung insgesamt nur dadurch unterscheiden, daß sie aus der DDR oder aus osteuropäischen Staaten in die Bundesrepublik gekommen sind und deshalb mit einer sehr geringen statistischen Wahrscheinlichkeit später einmal, falls sich entsprechende Sachverhalte ergeben sollten, als Auskunftspersonen in Betracht kommen können, ist mit generalklauselartig gefaßten gesetzlichen Befugnissen, die sich allgemein an der Erforderlichkeit zur Erfüllung näher spezifizierter Aufgaben orientieren, nicht zu rechtfertigen. Wie sich nicht zuetzt an der geringen Nutzungsquote erweist, stellt die Erfassung in ADOS eine vorsorgliche Maßnahme dar, die die Erfüllung von Aufgaben erleichtern soll, die sich erst bei künftigen Sachverhalten ergeben. Die Datei ADOS nähert sich damit stark einer Verarbeitung personenbezogener Daten auf Vorrat. Dies ist nur dort vertretbar, wo der Gesetzgeber für die *spezielle* Konfliktsituation entschieden hat, daß das Allgemeininteresse insoweit der informationellen Selbstbestimmung vorgehen soll.

d) Ein Teil der in ADOS gelangenden Daten stammt aus dem Notaufnahmeverfahren. Das von den Antragstellern im Rahmen dieses Verfahrens auszufüllende Formular enthält u. a. Fragen nach den Wohnanschriften der letzten zehn und den Arbeitgebern der letzten fünfzehn Jahre. Diese Angaben sind nicht im Sinne von § 9 Abs.2 BDSG als freiwillig ausgewiesen, sondern werden den Antragstellern obligatorisch abverlangt. Die Richtigkeit und Vollständigkeit aller Angaben ist durch Unterschrift zu versichern. Da nicht erkennbar ist, daß die geforderten Angaben für Zwecke des Aufnahmeverfahrens benötigt werden, habe ich den BMI schon vor Jahren aus Anlaß einer Prüfung in einem Aufnahmelager auf die datenschutzrechtlichen Bedenken hingewiesen. Der BMI hat darauf erwidert, daß er meinen Bedenken im Rahmen einer beabsichtigten Umstellung des Verfahrens Rechnung tragen wolle. Dazu ist es aber bis heute nicht gekommen. Ich habe deshalb daran erinnert.

Ich begrüße es, daß der BMI im Hinblick auf die politische Entwicklung in den Ostblockstaaten entschieden hat, die systematische Befragung von Aus- und Übersiedlern für ADOS und die Speicherung bereits erhobener Daten in ADOS vorläufig einzustellen, wie er mir Mitte Dezember mitgeteilt hat. Die endgültige Entscheidung soll danach noch mit den Ländern abgestimmt werden. Im Hinblick auf die datenschutz-

rechtlichen Mängel, mit denen die Datenerhebung belastet ist, und angesichts des schon angesprochenen grundsätzlichen Wandels des gesamten Umfeldes gehe ich davon aus, daß eine vollständige Bereinigung vorzunehmen sein wird.

19.3 Kontrolle bei der Abteilung III

Eine im Jahre 1983 beim Bundesamt für Verfassungsschutz durchgeführte datenschutzrechtliche Kontrolle der für die Beobachtung des Linksexstremimus zuständigen Abteilung III hatte schwerwiegende Mängel gezeigt (vgl. 6. TB S. 49f.). In den folgenden Jahren war daraufhin der Verkartungsplan, der die Informationsverarbeitung regelt, in weiten Teilen neu konzipiert worden. 1989 habe ich die Abteilung III erneut geprüft, um festzustellen, ob die Neuregelungen des Verkartungsplans greifen. Zu diesem Zweck wurden nach dem Zufallsprinzip 100 Akten ausgewählt, bei denen im Jahre 1988 zumindest eine neue NADIS-PZD-Fundstelle hinzugespeichert worden ist.

Das Ergebnis meiner Kontrolle war günstiger als bei der 1983 durchgeführten Kontrolle, zeigt aber immer noch Mängel auf. Es läßt sich statistisch wie folgt zusammenfassen:

— In 74 Fällen entsprach die Speicherung auch nach meiner Auffassung dem Verkartungsplan; darin waren auch solche enthalten, die durch Korrekturen am Datensatz bereinigt werden konnten, wobei die Berechtigung zur Speicherung nicht umstritten war.

— 16 Speicherungen wurden aus Anlaß der Kontrolle gelöscht. Darunter waren Speicherungen, die auch nach Auffassung des BfV von vornherein nicht hätten vorgenommen werden dürfen, und solche, bei denen eine Fortdauer der Speicherung im Zeitpunkt der Prüfung nicht mehr erforderlich war.

— In 9 weiteren Fällen war die Zulässigkeit der Speicherung nach meiner Auffassung zweifelhaft. Allerdings erschien auch die vom BfV vorgenommene Auslegung des Verkartungsplans vertretbar.

— In einem Fall, bei dem eine listenmäßige Mitteilung einer Polizeibehörde zu einer Vielzahl von Speicherungen geführt hatte, ist zwischenzeitlich ein Teil der konkreten Fälle gelöscht. Aus meiner Sicht hatte sich das BfV nicht in bezug auf jede betroffene Person davon überzeugt, daß die im Verkartungsplan für eine Speicherung verlangten tatsächlichen Voraussetzungen gegeben waren. Die Meinungsverschiedenheit über diese Frage besteht fort, so daß aus meiner Sicht weitere Fehler dieser Art nicht auszuschließen sind.

Im Rahmen der Neufassung des Verkartungsplans hatte ich Wert darauf gelegt, daß im Falle einer zeitlichen Verlängerung einer Speicherung die Ziffer des Verkartungsplans, auf die diese Maßnahme gestützt wird, in der Akte vermerkt wird. Der neue Verkartungsplan sieht eine solche Verpflichtung vor. In einer Reihe von Fällen war diese Bestimmung aber nicht beachtet worden. Das BfV hat eine Korrektur zugesichert.

Ich habe weiterhin festgestellt, daß aufgrund von Familienanzeigen im Presseorgan einer bestimmten als verfassungsfeindlich bewerteten Partei personenbezogene Informationen gespeichert worden waren. Das Bundesamt hat diese Praxis inzwischen abgestellt.

Aufgrund weiterer Feststellungen, die hier aus Gründen des Geheimschutzes nicht dargelegt werden können, habe ich weitere Präzisierungen im Verkartungsplan angeregt. Der BMI ist bisher nur einem kleinen Teil dieser Anregungen gefolgt.

Die politischen Veränderungen in Deutschland und Europa werden sich auch auf die Verarbeitung personenbezogener Daten beim Verfassungsschutz auswirken. Dies wird Anlaß geben, insbesondere den Verkartungsplan für die Abteilung III sehr bald erneut zu überarbeiten.

20 Verteidigung

20.1 Psychologische Verteidigung

Eine der Psychologischen Verteidigung gewidmete Sendung des Fernseh-Magazins Monitor vom 17. Januar 1989 hat mir Anlaß zu Informationsbesuchen und datenschutzrechtlichen Kontrollen bei für die Psychologische Verteidigung zuständigen Stellen im Geschäftsbereich des Bundesministers der Verteidigung gegeben. Dabei habe ich beim Streitkräfteamt als Dateien zu bewertende Sammlungen personenbezogener Daten festgestellt. Es handelte sich um

— eine Kartei von Vereinigungen, die sich an der geistig-politischen Auseinandersetzung mit der Verteidigung beteiligen, sowie

— einen Aktenordner mit Exponenten von Vereinigungen, die sich an der geistig-politischen Auseinandersetzung mit der Verteidigung beteiligen.

Gesammelt wurden Daten und Äußerungen von Personen, die aus der Sicht der Psychologischen Verteidigung als besonders bedeutsam angesehen wurden. Dabei wurden auch Daten gespeichert, die in keinerlei Beziehung zur Aufgabe der Psychologischen Verteidigung standen, so z. B. das im Zusammenhang mit anderen Daten gespeicherte Merkmal „alleinerziehende Mutter", Angaben über Berufsausbildung und berufliche Tätigkeit sowie Beschäftigungsstelle, die private Adresse, das genaue Geburtsdatum und der Geburtsort.

Ich habe die Führung dieser Dateien in der bisherigen Form wegen Verstoßes gegen datenschutzrechtliche Vorschriften gemäß § 20 BDSG förmlich beanstandet. Gründe hierfür waren das Fehlen einer Rechtsgrundlage und die mangelnde Erforderlichkeit für die rechtmäßige Erfüllung der Aufgaben des Streitkräfteamtes (Verstoß gegen § 9 Abs. 1 BDSG), die langjährige Nichtaufnahme der in den Dateien enthaltenen Daten in die Dateienübersicht (Verstoß gegen § 15 Nr. 1 BDSG) und das Unterlassen der Veröffentlichung der Dateien (Verstoß gegen § 12 BDSG).

Etwaige Anhaltspunkte dafür, daß Dienststellen der Psychologischen Verteidigung personenbezogene Daten mit verdeckten oder nachrichtendienstlichen Mitteln erheben, haben sich bei meiner Kontrolle nicht ergeben.

Der BMVg hat mich von Anfang an bei der Aufklärung des Sachverhalts unterstützt. Seine Stellungnahme auf meine Beanstandung enthält den Kernsatz: „PSV-Maßnahmen gegenüber der eigenen Bevölkerung sind als Einsatzmodalität der Streitkräfte im Frieden durch den Verfassungsauftrag zur Landesverteidigung *nicht gedeckt.*" Er bestätigt damit, daß es für eine Datenverarbeitung zum Zwecke solcher Maßnahmen gegenüber der eigenen Bevölkerung keine Erforderlichkeit im überwiegenden Allgemeininteresse und auch keine Rechtsgrundlage gibt. Der BMVg hat die Weiterführung der von mir beanstandeten Dateien umgehend eingestellt. Im Einvernehmen mit mir standen diese wegen vieler Anfragen von Bürgern noch bis Ende September 1989 im BMVg ausschließlich zu dem Zwecke zur Verfügung, Betroffenen gemäß § 13 BDSG auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen. Danach sind die Dateien vernichtet worden.

Meine Beanstandung stellt eine Auswertung von Publikationen im Rahmen der der Bundesregierung und den Ressorts zustehenden Informationskompetenz nicht in Frage. Als Rechtsgrundlage für eine Datenverarbeitung mit dieser Zweckbestimmung — geltend für alle Bundesressorts — ist Artikel 65 Satz 2 des Grundgesetzes anzusehen, wonach jeder Bundesminister innerhalb der Richtlinien des Bundeskanzlers seinen Geschäftsbereich selbständig und unter eigener Verantwortung leitet. Zugleich habe ich deutlich gemacht, daß auf dieser Grundlage nur Daten von Personen gespeichert werden dürfen, die sich mit dem Willen an der öffentlichen Diskussion beteiligen, daß ihr Wort auch dokumentiert wird und einen nicht bestimmten Kreis von Adressaten erreicht. Dabei habe ich unterstrichen, daß der Umfang zulässiger Speicherung personenbezogener Daten durch den Zweck begrenzt wird, Bedeutung und Wirkungskraft von Argumenten zu bestimmen. Diese Rechtslage muß auch in bezug auf die Stelle, der eine Datenverarbeitung zu diesem Zweck übertragen worden ist, deutlich werden. Eine Datenverarbeitung zu dem beschriebenen Zweck durch ein Fachreferat im Bereich der Psychologischen Verteidigung ist deshalb abzulehnen. Der Dialog mit dem BMVg, bei dem es auch um eine Neufassung der Zentralen Dienstvorschrift für die Psychologische Verteidigung geht, ist noch nicht abgeschlossen.

20.2 Auskünfte des Instituts für Wehrmedizinalstatistik und Berichtswesen

Im Institut für Wehrmedizinalstatistik und Berichtswesen werden alle ärztlichen Unterlagen, die in Verbindung mit dem Wehrdienst entstehen, zentral archiviert, um bei Anfragen Auskünfte erteilen zu können, entweder an den Betroffenen oder — mit seinem ausdrücklichen schriftlichen Einverständnis — auch an Dritte.

In einem mir von einem Petenten geschilderten Fall hat dieser um die Übersendung von Fotokopien seiner ärztlichen Unterlagen gebeten. Trotz mehrmaliger Anfragen wurde ihm dies vom Institut verweigert. Zunächst hat das Institut ihn aufgefordert, einen Arzt zu benennen, dem die Unterlagen übersandt werden sollten. Dann verwies es ihn auf die Möglichkeit, die Unterlagen im Institut einzusehen. Dies akzeptierte der Petent jedoch nicht; er beklagte sich über die „Geheimnistuerei" und wandte sich an mich.

In der erbetenen Stellungnahme hat mir der BMVg erklärt, daß bisher die Unterlagen grundsätzlich dem weiterbehandelnden Arzt zugesandt wurden, damit dieser seinem Patienten bei Bedarf Erläuterungen geben kann. Dieses Verfahren habe sich in der Vergangenheit bewährt. Nunmehr ist der BMVg jedoch — wie er mir mitgeteilt hat — zu der Auffassung gelangt, daß in den Fällen, in denen der Petent auf der Übersendung von Kopien an ihn selbst besteht, eine Weigerung mit der heutigen Rechtsauffassung nicht mehr vereinbar ist. Er hat deshalb das Institut für Wehrmedizinalstatistik und Berichtswesen angewiesen, dem Petenten Kopien aller Gesundheitsunterlagen zu übersenden und bei entsprechenden Anforderungen künftig in gleicher Weise zu verfahren. Ich befürworte diese Entscheidung.

20.3 Weitergabe von Adressen an Dritte

In einer weiteren Eingabe rügte ein Petent, der BMVg habe Namen und Anschriften von Offizieren der Reserve ohne deren Einwilligung an einen privaten Zeitschriftenverlag weitergegeben. Dem Petenten wurde die Zeitschrift mit einem Anschreiben des BMVg übersandt, in dem angekündigt wurde, daß in Führungsfunktionen beorderte Angehörige der Reserve in die Versorgung mit Zeitschriften der Truppeninformation einbezogen werden sollen. Dank einer Initiative des privaten Verlages werde die in Zusammenarbeit mit dem BMVg verlegte Zeitschrift den Reservisten kostenfrei zur Verfügung gestellt.

Der BMVg hat dargelegt, daß er dem Zeitschriftenverlag die Namen und Anschriften von 2 000 Offizieren der Reserve zur Verfügung gestellt hat. Die Einwilligung der Adressaten zur Übermittlung ihrer personenbezogenen Daten sei nicht eingeholt worden, weil das zuständige Referat davon ausgegangen sei, daß schutzwürdige Belange der Betroffenen nicht beeinträchtigt würden. Ferner sei die Aktion von der überwiegenden Zahl der belieferten Reserveoffiziere als in ihrem Interesse liegend begrüßt worden. Der Verlag habe sich schriftlich zur vertraulichen Behandlung der Daten verpflichtet.

Ergänzend hat der BMVg erklärt, ihm seien keine weiteren Fälle bekannt, in denen Dienststellen seines Ressorts Daten von aktiven Soldaten oder von Angehörigen der Reserve an Zeitschriftenverlage oder andere entsprechende Stellen weitergegeben haben.

Mit gleichem Schreiben hat mir der BMVg mitgeteilt, daß die beschriebene Aktion inzwischen eingestellt und auf seine Veranlassung die personenbezogenen Daten bei dem Verlag wieder gelöscht worden sind. Ferner hat er mir versichert, bei der Realisierung der

vorgesehenen regelmäßigen Einbeziehung der Reservisten in die Truppeninformation künftig die Bestimmungen des Bundesdatenschutzgesetzes zu beachten. Ich gehe dementsprechend davon aus, daß künftig das Einverständnis der Betroffenen eingeholt wird, bevor deren Name und Anschrift an einen Zeitschriftenverlag weitergegeben werden.

20.4 Ergebnisse meiner datenschutzrechtlichen Kontrolle beim Militärischen Abschirmdienst

Die Gespräche mit dem BMVg über die Konsequenzen, die nach meiner datenschutzrechtlichen Querschnittskontrolle beim Militärischen Abschirmdienst (MAD) im Jahre 1988 zu ziehen sind, wurden im Berichtsjahr mit weiteren konkreten Ergebnissen fortgesetzt. Der MAD wird seine Arbeitsweisung Nr. 5, in der u. a. die Fristen für die Speicherung personenbezogener Daten in Dateien des MAD geregelt sind, noch einmal überarbeiten. Er wird hierbei in zwei wichtigen Punkten meinen Vorschlägen folgen:

a) Konnte durch die Ermittlungen des MAD der Verdacht sicherheitsgefährdender Bestrebungen unmittelbar gegen die Bundeswehr zweifelsfrei ausgeräumt werden, so wird die Frist für die Aufbewahrung der entsprechenden Unterlagen, die derzeit zehn Jahre beträgt, verkürzt. Einzelheiten sind noch festzulegen.

b) Eine wichtige zugesagte Neuerung betrifft die Speicherung von Daten über Personen, die extremistischen Organisationen angehören, während ihrer Zugehörigkeit zur Bundeswehr aber keine Bestrebungen unmittelbar gegen die Bundeswehr unternehmen. Da letzteres u. a. Voraussetzung für die Zuständigkeit des MAD ist, habe ich dessen Praxis kritisiert, in solchen Fällen Daten auch dann noch in Dateien zu speichern, wenn die Betroffenen die Bundeswehr bereits verlassen haben. Der BMVg hat nunmehr zugesagt, daß in diesen Fällen die Daten bei Beendigung der Bundeswehrzugehörigkeit gelöscht werden. Dies dürfte spürbare Auswirkungen auf den Datenbestand im „Abwehrbereich verfassungsfeindliche Kräfte" haben. Da in den vergangenen Jahren kaum unmittelbar gegen die Bundeswehr gerichtete extremistische Bestrebungen bekannt geworden sind, betraf ein Großteil der dort gespeicherten Daten Personen, für die jedenfalls nach Beendigung der Bundeswehrzeit allenfalls die Verfassungsschutzbehörden, nicht aber der MAD zuständig war.

Der BMVg will meiner Kritik an der langen Dauer der Bereinigungsarbeiten beim MAD Rechnung tragen. Er strebt eine Bereinigung der gesamten Datenbestände der Abwehrbereiche 1 (Sicherheitsüberprüfung) und 2 (verfassungsfeindliche Kräfte) bis Ende 1990 an. Auch im Abwehrbereich 3 (Spionageabwehr) werden sämtliche Datenspeicherungen überprüft; dies soll bis auf einige Restbestände von ca. 20 % bis Ende 1990 erledigt sein. Der Zeitraum für die noch anstehenden Bereinigungen würde sich damit von ursprünglich acht bis zehn Jahren auf im wesentlichen zwei Jahre reduzieren. Dies entspräche meinem Vorschlag. Die Datenbestände des MAD werden sich damit vermutlich noch einmal beträchtlich verringern.

Es wäre zu wünschen, daß auch die anderen Sicherheitsbehörden ihre gesamten Datenbestände unter datenschutzrechtlichen Gesichtspunkten durchforsten und bereinigen.

Der BMVg hat mir in seiner Stellungnahme ferner mitgeteilt, daß einige kleinere Dateien bei einzelnen MAD-Gruppen, deren Erforderlichkeit ich hinterfragt hatte, nicht mehr weiter betrieben und vernichtet werden.

Ich hatte in meinem Kontrollbericht auch Kritik daran geäußert, daß in einzelnen Fällen bei Befragungen durch den MAD Mitarbeiter von Verfassungsschutzbehörden anwesend waren, ohne daß der Betroffene dies wußte. Der BMVg stimmt mit mir darin überein, daß dies nicht zulässig ist. Eine zunächst vorgesehen entsprechende Klarstellung in den maßgeblichen Vorschriften, die ich für geboten halte, hat er nunmehr aber abgelehnt.

Kritik hatte ich in meinem Kontrollbericht wie auch in meinem Elften Tätigkeitsbericht (S. 71) an dem Umfang geübt, in dem der MAD Daten, die im Rahmen einer Sicherheitsüberprüfung erhoben wurden, an Verfassungsschutzbehörden weiterübermittelt. Die vom BMVg angekündigte Überarbeitung der entsprechenden Vorschrift ist mir bislang noch nicht zugegangen.

Nicht zufriedenstellend ist bislang die Stellungnahme des BMVg zur Frage des Einsatzes nachrichtendienstlicher Mittel durch den MAD. Ich hatte kritisiert, daß nach meinem Eindruck die Schwelle für die Durchführung von Operationen mit nachrichtendienstlichen Mitteln beim MAD zu niedrig ist. Der BMVg macht geltend, wegen der geringen Zahl der in meine Überprüfung einbezogenen Vorgänge komme meinen Aussagen kein repräsentativer Charakter zu. Ich werde mich der Angelegenheit weiter annehmen.

21 Wirtschaftsverwaltung

21.1 Änderung gewerberechtlicher Vorschriften

Das geltende Gewerbe- und Wirtschaftsverwaltungsrecht genügt in weiten Teilen nicht den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts. So besteht Anpassungsbedarf bei

— Regelungen, die recht unbestimmte Ermächtigungen für die Verwaltung zum Erlaß von Rechtsverordnungen enthalten und zum Erlaß von Vorschriften über die Erhebung oder Verarbeitung personenbezogener Daten Gewerbetreibender genutzt werden: § 34 Abs. 2 Nr. 4, § 34 a Abs. 2, § 34 c Abs. 3 und § 38 der Gewerbeordnung sowie § 22 und § 30 des Gaststättengesetzes.

— Regelungen, die eine Anzeigepflicht von Gewerbetreibenden begründen, ohne zugleich die Voraussetzungen der Übermittlung der so gewonnenen Daten (z. B. aus dem Gewerberegister) an dritte Stellen (u. a. Handwerkskammern und Industrie- und Handelskammern) zu bestimmen: § 14 und § 55 c der Gewerbeordnung. In diesem Zusammenhang ist auch die in § 35 Abs. 4 der Gewerbe-

ordnung vorgesehene Anhörung von staatlichen Aufsichtsbehörden, Prüfungsverbänden, Industrie- und Handelskammern sowie Handwerkskammern im Untersagungsverfahren zu nennen; sie läßt ungeregelt, welche Unterlagen über den Gewerbetreibenden bei dieser Anhörung vorzulegen sind.

— Regelungen, die den Umfang der Datenerhebung, z. B. im Rahmen einer Zuverlässigkeitsprüfung, nicht hinreichend bestimmen: § 4 des Gaststättengesetzes und § 14 des Personenbeförderungsgesetzes.

Angesichts dieser datenschutzrechtlichen Defizite begrüße ich die Initiative des Bund-Länder-Ausschusses „Gewerberecht", mit einem Entwurf eines Gesetzes zur Änderung gewerberechtlicher Vorschriften erstmalig ausreichende Rechtsgrundlagen für die gewerberechtliche Datenverarbeitung schaffen zu wollen. Der Gesetzentwurf begegnet jedoch in seiner ersten Fassung noch datenschutzrechtlichen Bedenken. So enthalten einige Regelungen, darunter die zentrale Vorschrift des neuen § 11 Gewerbeordnung, unklare und unvollständige Formulierungen zur Datenerhebung und Datenübermittlung, die den Datenfluß gegenüber der jetzigen Verfahrensweise sogar noch weniger eingrenzen würden.

Gemeinsam mit den wegen der landesrechtlichen Auswirkungen des Gesetzentwurfs zuständigen Landesbeauftragten für den Datenschutz werde ich darauf hinwirken, daß bei den weiteren Beratungen den notwendigen datenschutzrechtlichen Empfehlungen Rechnung getragen wird.

21.2 Bundesaufsichtsamt für das Versicherungswesen

Im vergangenen Jahr habe ich über eine Kontrolle beim Bundesaufsichtsamt für das Versicherungswesen berichtet (11. TB S. 76). Die von mir in einigen Aufgabenbereichen festgestellten datenschutzrechtlichen Mängel hat der BMF bislang nicht ausgeräumt.

— Die Sammlung von Daten über Vorstandsmitglieder von Versicherungsgesellschaften entbehrt einer ausreichenden rechtlichen Grundlage. Die vom Bundesminister der Finanzen herangezogenen Vorschriften des Versicherungsaufsichtsgesetzes (§§ 8, 81, 87), die für Vorstandsmitglieder eine Eignungsbeurteilung vorsehen, ehe ihrem Unternehmen die Erlaubnis zum Geschäftsbetrieb erstmalig erteilt wird, sind außerordentlich unscharf und als Datenerhebungsvorschrift ungeeignet. Kriterien wie Ehrbarkeit, fachlich genügende Vorbildung und „sonst erforderliche Eigenschaften und Erfahrungen" lassen dem Betroffenen nicht erkennbar werden, in welchem Maß er dem Bundesaufsichtsamt persönliche Lebenssachverhalte vor seiner Bestellung zum Vorstandsmitglied offenbaren muß. Ein weiterer Mangel dieses „Vorstandsregisters" ist es, daß auch für die laufende Kontrolle der Ehrbarkeit und Eignung einmal bestellter Vorstandsmitglieder oder später neu eintretender Vorstandsmitglieder das Versicherungsaufsichtsgesetz keine normenklare Rechtsgrundlage bietet.

— Bei meiner Kontrolle hatte ich festgestellt, daß das Bundesaufsichtsamt in einer Kartei über Veruntreuungen im Versicherungsaußendienst auch personenbezogene Daten über Außendienstmitarbeiter von Versicherungsunternehmen sammelt, wenn diese Mitarbeiter von Versicherungsunternehmen verdächtigt werden, Veruntreuungen in Höhe von mehr als 5 000,— DM begangen zu haben. Die betroffenen Außendienstmitarbeiter erhalten seitens des Amtes keine Gelegenheit, sich vor der Datenspeicherung zu der Beschuldigung zu äußern. Die Datenübermittlung erfolgt aufgrund eines Rundschreibens des Bundesaufsichtsamtes aus dem Jahre 1973. Der Bundesminister der Finanzen sieht auch diese Datenerhebung durch § 81 Versicherungsaufsichtsgesetz gedeckt; er vertritt im übrigen die Auffassung, daß „im Rahmen des Allgemeininteresses an einem sauberen und vertrauenswürdigen Außendienst das Recht des einzelnen auf Datenschutz zurücktreten muß." Ich habe deutlich gemacht, daß für die Verarbeitung personenbezogener Daten von Außendienstmitarbeitern, die zudem ohne deren Kenntnis erfolgt, keine ausreichende Rechtsgrundlage ersichtlich ist; § 81 Versicherungsaufsichtsgesetz kann eine klare Ermächtigung dazu nicht entnommen werden. Meinen gravierenden datenschutzrechtlichen Bedenken hat der Bundesminister der Finanzen bislang nicht Rechnung getragen.

Im Zusammenhang mit Datenschutzproblemen der privaten Versicherungswirtschaft begrüße ich die Bereitschaft des Bundesministers der Finanzen, mich im Vorfeld von Bedingungs- und Klauselgenehmigungen durch das Bundesaufsichtsamt für das Versicherungswesen zu unterrichten, damit ich auch insoweit meiner Beratungsaufgabe nachkommen kann. Ich gehe davon aus, daß diese Unterrichtung alle Fälle betrifft, in denen das Amt Regelungen treffen will, die die Verarbeitung personenbezogener Daten durch die Versicherungsunternehmen betreffen oder sich darauf auswirken.

21.3 Bundesaufsichtsamt für das Kreditwesen

Beim Bundesaufsichtsamt für das Kreditwesen habe ich die automatisierte Datenverarbeitung sowie den damit verbundenen Umgang mit personenbezogenen Daten bei der Erledigung der Fachaufgaben des Amtes kontrolliert. Besondere Mängel habe ich nicht festgestellt; lediglich in den Bereichen der organisatorischen Sicherstellung des Datenschutzes und der Datensicherung bestand Veranlassung, auf datenschutzrechtliche Defizite hinzuweisen. So enthielt z. B. die gemäß § 15 BDSG zu führende Dateiübersicht nicht sämtliche im Amt vorhandenen Dateien; dem internen Datenschutzbeauftragten waren jedoch die in der Übersicht nicht aufgeführten Dateien bekannt.

Nach Auskunft des Bundesaufsichtsamtes sind die bei der Prüfung zutage getretenen organisatorischen

und technischen Mängel inzwischen beseitigt worden.

Im Rahmen seiner Aufgabenwahrnehmung verfügt das Bundesaufsichtsamt für das Kreditwesen über einen online-Zugriff auf einige Datenbanken der Deutschen Bundesbank. Diese Datensammlungen enthalten u. a. Informationen über Geschäftsleiter von Kreditinstituten sowie die der Bundesbank nach den Vorschriften des Kreditwesengesetzes zu meldenden Groß- und Millionenkreditnehmer. Das Bundesaufsichtsamt plant, in nächster Zeit an etwa 90 Arbeitsplätzen, die über sämtliche Abteilungen des Amtes verteilt sind, Terminals einzurichten, die den gleichberechtigten Zugriff auf die genannten Datenbestände der Deutschen Bundesbank bieten. Ich habe den Bundesminister der Finanzen gebeten, mir zu erläutern, inwieweit es für die Aufgabenwahrnehmung der für unterschiedliche Bereiche des Kreditwesens (z. B. Genossenschaftsbanken und Hypothekenbanken) zuständigen Bediensteten erforderlich ist, über Informationen zu sämtlichen Bereichen der Kreditwirtschaft zu verfügen.

Eine Antwort des Bundesministers für Finanzen hat mich vor Redaktionsschluß dieses Berichtes noch nicht erreicht.

21.4 Förderung der Unternehmensberatung

Über datenschutzrechtliche Probleme bei der Förderung von Unternehmensberatungen durch das Bundesamt für Wirtschaft habe ich berichtet (10. TB S. 87 und 11. TB S. 75).

Der Bundesminister für Wirtschaft hat mit der seit Januar 1990 geltenden Neufassung der Richtlinien über die Förderung von Unternehmensberatungen für kleine und mittlere Unternehmen nunmehr meinen datenschutzrechtlichen Anregungen Rechnung getragen. Die Richtlinien enthalten sämtliche vom Bundesminister für Wirtschaft im Vorjahr angekündigten Verbesserungen (11. TB S. 75). Hervorzuheben ist, daß mit der vom Unternehmensberater erbetenen Einwilligung erstmals eine tragfähige Rechtsgrundlage für die Speicherung seiner Daten durch das Bundesamt für Wirtschaft geschaffen worden ist. Der Wortlaut der Einwilligungserklärung bringt auch zum Ausdruck, daß Beraterdaten von den Leitstellen nur entgegengenommen und an das Bundesamt für Wirtschaft weitergeleitet werden dürfen. Ich begrüße in diesem Zusammenhang die an die Leitstellen gerichtete unmißverständliche Aufforderung des Bundesamtes für Wirtschaft, die eingereichten Antragsunterlagen nach Bearbeitung weiterzuleiten und hiervon keine Kopien zu fertigen und zurückzubehalten.

21.5 Gesetzentwürfe zur Verbesserung der Außenwirtschaftskontrolle

Die Gesetzentwürfe der Bundesregierung zur Verbesserung der Außenwirtschaftskontrolle bewirken eine erhebliche Vorverlagerung der polizeilichen und zollfahndungsmäßigen Kontrolle. Sie schränken damit den Grundsatz der Trennung des normalen Verwaltungsvollzugs von der polizeilichen Kontrolle deutlich ein. Ob solche weitgehenden gesetzlichen Regelungen geschaffen werden sollen, ist letztlich eine politische Entscheidung. Aus meiner Sicht ist aber zu fordern, daß solche Regelungen so klar wie möglich im Gesetz formuliert werden. Von hieraus habe ich es begrüßt, daß sich der Bundesminister für Wirtschaft bereiterklärt hat, in den Entwurf zu § 45 Außenwirtschaftsgesetz die datenschutzrechtlich erforderliche Regelung des automatisierten Abrufverfahrens aufzunehmen. Nach längeren Verhandlungen hat der BMWi auch meine weiteren Anregungen aufgegriffen. So sollen die Behörden, an die das Zollkriminalinstitut personenbezogene Daten, die auch dem Steuergeheimnis unterliegen können, weiterleiten darf, in einer Rechtsverordnung benannt und auch der Umfang der Datenübermittlung soll in dem vorgesehenen neuen § 24a Atomgesetz hinreichend konkretisiert werden.

Bislang liegen mir zum Konzept der beim Zollkriminalinstitut vorgesehenen Ausfuhrkontrolldatenbank KOBRA keine ausreichenden Informationen vor, die eine Beurteilung der konkreten Aufgaben und etwaigen datenschutzrechtlichen Risiken dieses Informationssystems erlauben würden.

Überhaupt ist den Vorüberlegungen zu den Gesetzentwürfen zu entnehmen, daß das Gesamtkonzept der Bundesregierung offenbar auch einen intensivierten und routinemäßigen Datenaustausch zwischen dem Bundesamt für Wirtschaft, dem Bundeskriminalamt und dem Bundesnachrichtendienst vorsieht, ohne daß hierzu Vorschläge zur Gesetzesänderung gemacht werden. Weil mir auch Einzelheiten dieser vorgesehenen Zusammenarbeit nicht bekannt sind, sehe ich mich insoweit zu einer abschließenden Bewertung des Gesetzgebungsvorhabens außerstande. Dies habe ich dem Ausschuß für Wirtschaft des Deutschen Bundestages und dem BMWi mitgeteilt.

22 Umweltschutz

22.1 Gesetzentwurf zur Umsetzung der EG-Richtlinie über die Umweltverträglichkeitsprüfung

Der Deutsche Bundestag hat im November das Gesetz zur Umsetzung der Richtlinie des Rates der EG vom 27. Juni 1985 über die Umweltverträglichkeitsprüfung bei bestimmten öffentlichen und privaten Projekten (UVPG) verabschiedet.

Die datenschutzrechtliche Problematik dieses Gesetzes liegt darin, in den verwaltungsbehördlichen Verfahren, die der Entscheidung über die Zulässigkeit von Vorhaben dienen und die unter Einbeziehung der Öffentlichkeit durchgeführt werden, einen angemessenen Ausgleich zwischen dem Geheimhaltungsinteresse der Verfahrensbeteiligten und dem Informationsinteresse der Öffentlichkeit zu schaffen.

Aufgrund meiner Empfehlungen in den Ausschußberatungen macht der Wortlaut des Gesetzes (§ 10) nunmehr deutlich, daß im UVP-Verfahren nicht nur die eng gefaßten, im staatlichen Interesse stehenden

Rechtsvorschriften über Geheimhaltung zu berücksichtigen sind, sondern auch der Schutz personenbezogener Daten zu gewährleisten ist.

Ich begrüße insbesondere den zum UVPG ergangenen Beschluß des Deutschen Bundestages, die Bundesregierung zu bitten, durch Änderung der einschlägigen Umweltgesetze sicherzustellen, daß in UVP-Verfahren bei der Offenbarung personenbezogener Daten Rechte Dritter und des Vorhabenträgers nicht beeinträchtigt werden. Zur Erreichung dieses Zieles wird die Bundesregierung gebeten, die erforderlichen Gesetzentwürfe vorzulegen. Mit diesem Beschluß, der meine Empfehlungen berücksichtigt, wird auf die noch ausstehende Lösung eines wichtigen datenschutzrechtlichen Anliegens hingewiesen.

22.2 Gefahrstoffdatenbank

Der Bundesrat hat in seiner Stellungnahme zum Gesetzentwurf der Bundesregierung zur Änderung des Chemikaliengesetzes mit einem Ergänzungsvorschlag gefordert, in diesem Gesetz die rechtliche Grundlage für den Aufbau einer gemeinsamen Gefahrstoffdatei der Länder zu schaffen. Diese Datei solle der Überwachungstätigkeit und der Unfallverhütung durch die zuständigen Aufsichtsbehörden und Berufsgenossenschaften dienen.

Weil die zur Datei zu meldenden Daten auch personenbezogene Herstellerangaben sowie Betriebs- und Geschäftsgeheimnisse betreffen können, habe ich in Ressortbesprechungen und Stellungnahmen gegenüber dem Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit empfohlen, den Vorschlag des Bundesrates datenschutzgerecht zu fassen. So habe ich zur Verhinderung eines unkontrollierbaren Datenflusses angeregt, den Kreis der an der Datenübermittlung beteiligten Behörden nach Aufgabenbereichen zu konkretisieren und die Zweckbestimmung der Datenverwendung deutlich werden zu lassen.

Ich bedauere, daß die Bundesregierung meine Vorstellungen in ihrer Gegenäußerung zur Stellungnahme des Bundesrates nicht aufgegriffen hat. Sie sieht vielmehr für die beim Aufbau einer Gefahrstoffdatenbank notwendigen Datenverarbeitungsvorgänge in den geltenden Datenschutzgesetzen eine ausreichende rechtliche Grundlage. Ihren Gegenvorschlag, der Datenübermittlungen im Wege der Amtshilfe vorsieht, halte ich aus datenschutzrechtlicher Sicht für unzureichend. Eine Datenübermittlung im Wege der Amtshilfe erfolgt nur auf einzelne Ersuchen hin; sie kann keine ausreichende Grundlage für eine zum Aufbau einer Gefahrstoffdatenbank erforderliche regelmäßige Datenübermittlung sein.

23 Landwirtschaft

— Ernährungssicherstellungsgesetz und Ernährungsvorsorgegesetz —

Der Bundesminister für Ernährung, Landwirtschaft und Forsten hatte mich bereits im Jahr 1988 an der Vorbereitung der im September von der Bundesregierung beschlossenen Entwürfe eines Zweiten Gesetzes zur Änderung des Ernährungssicherstellungsgesetzes und eines Ernährungsvorsorgegesetzes beteiligt. So konnte das datenschutzrechtliche Problem der Gesetzentwürfe, die auf dem Ernährungssektor typischen Informationsbedürfnisse der zuständigen Behörden trotz Unvorhersehbarkeit von Krisenentwicklungen einzugrenzen und inhaltlich zu umschreiben, befriedigend gelöst werden. Ich begrüße es, daß die Gesetzentwürfe meine Empfehlungen weitgehend berücksichtigen und Art und Umfang der zu übermittelnden personenbezogenen Daten normenklar festlegen.

24 Datensicherung

Während die Notwendigkeit, bei der automatisierten Datenverarbeitung stets auch Fragen der Sicherheit zu berücksichtigen, in den letzten Jahren nur zögerlich akzeptiert wurde, ist das Sicherheitsbewußtsein im Berichtsjahr erheblich gewachsen. Hauptursache dafür war die Aufdeckung eines Falles, in dem Hacker ihre Kenntnisse und Fähigkeiten, mehr noch aber die Nachlässigkeiten einiger Betreiber und Benutzer von DV-Anlagen zu Spionagezwecken verwertet und dafür namhafte Beträge erhalten hatten.

Wegen der weit verbreiteten Sorglosigkeit und des daraus resultierenden Fehlens einer wirksamen Eigenkontrolle kann weder ausgeschlossen werden, daß weitere Fälle von so umfassender „Selbstbedienung" aus fremden Computern vorgekommen sind, noch, daß inzwischen neue erfolgreiche Angriffe unternommen wurden. Hoffentlich beeinflußt die öffentliche Behandlung dieses Falles das Bewußtsein der Datenverarbeiter so nachhaltig, daß Sicherheit der Datenverarbeitung zu einem ernsthafter als bisher verfolgten Arbeitsziel wird. Noch ist die Praxis defizitär, wie die Ergebnisse der Prüfungen durch den Bundesrechnungshof (s. Nr. 6.6.2 der Bemerkungen des BRH 1989 zur Haushalts- und Wirtschaftsführung, Bundestagsdrucksache 11/5383) wie meiner eigenen, im Berichtsjahr aus Kapazitätsgründen jedoch kaum noch durchgeführten Kontrollen von Rechenzentren und großen DV-Systemen der Verwaltung des Bundes zeigen. Es ist aber hervorzuheben, daß die Ernsthaftigkeit des Problems der sicheren Datenverarbeitung erkannt wurde (s. dazu nachfolgend 24.1) und damit Hinweise auf Risiken nicht mehr als unbegründete Fantasien abgetan werden. Sicher kam hier auch noch hinzu, daß durch den zunehmenden Einsatz von Rechnern den Verantwortlichen in den Behörden deutlich wurde, in welchem Maße die Erfüllung der Aufgaben von einer funktionierenden und von ihnen beherrschbaren Datenverarbeitung abhängig geworden ist.

Als neues und eher noch weniger beherrschtes Risiko ist seit einigen Jahren der Einsatz von Arbeitsplatzcomputern hinzugekommen. Wenn diese Geräte untereinander und mit anderen DV-Systemen vernetzt werden, und damit der Mißbrauch nicht mehr den physischen Zugang zum einzelnen Gerät voraussetzt, werden für eine Vielzahl von Stellen neue Probleme auftreten, deren Lösung zwar möglich ist, aber we-

sentlich mehr Aufwand verlangt, als bisher geleistet wird.

Deshalb begrüße ich die Entscheidung des Bundesministers der Verteidigung, in die Zentrale Dienstvorschrift 2/30 „Sicherheit in der Bundeswehr" Regelungen zur Herstellung und Erhaltung der Sicherheit im Bereich der Datenverarbeitung aufzunehmen. Danach hat jede Dienststelle einen Sicherheitsbeauftragten/Sicherheitsoffizier und bei Bedarf einen DV-Sicherheitsbeauftragten zu bestellen. Der Sicherheitsbeauftragte ist u. a. für die Absicherung der Dienststelle einschließlich der Überwachung der Durchführung der dafür erforderlichen Maßnahmen zuständig; dazu gehören aus der Sicht des Datenschutzes auch Maßnahmen der Zugangs- oder Abgangskontrolle. Der DV-Sicherheitsbeauftragte überwacht u. a. die Durchführung aller Bestimmungen zum Herstellen und Erhalten der DV-Sicherheit, überprüft DV-Systeme, wirkt bei deren Freigabe mit und arbeitet mit der Stelle zusammen, die zur Wahrnehmung der Aufgaben nach dem Bundesdatenschutzgesetz beauftragt ist (sofern er nicht selbst mit diesen Aufgaben betraut ist). Beide Beauftragte haben ein unmittelbares Vortragsrecht beim Dienststellenleiter. Der BMVg hat durch diese Regelungen deutlich gemacht, daß sichere Datenverarbeitung vor allem eigens dafür eingesetztes aber auch entsprechend ausgebildetes Personal erfordert. Dieses Personal muß noch zur Verfügung gestellt und geschult werden; aus meiner Sicht hat der BMVg damit aber die wesentlichen Grundlagen für eine richtige Struktur zur Organisation der Datensicherheit gelegt.

Diese Entscheidung des BMVg zeigt wieder einmal die weitgehende Identität von Maßnahmen zur Sicherung personenbezogener Daten und zur Sicherheit der Datenverarbeitung im Interesse der Aufgabenwahrnehmung. Mit Blick auf Maßnahmendefizite in diesem Bereich bei den meisten anderen Behörden sollte dieses Beispiel Schule machen.

24.1 Aktivitäten der Bundesregierung

Seit einigen Jahren arbeitet der Interministerielle Koordinierungsausschuß für die Sicherheit in der Informationstechnik (ISIT), in dem ich mitwirke, an Projekten, die zu mehr Sicherheit in der Datenverarbeitung und Datenübertragung beitragen sollen. Diese Bemühungen führten erstmals im Berichtsjahr zu deutlich sichtbaren Ergebnissen.

Als langfristig am wirksamsten dürfte sich dabei die allerdings noch nicht abgeschlossene Umwandlung der Zentralstelle für das Chiffrierwesen (ZfCh), die früher fast ausschließlich für militärische, geheimdienstliche und vergleichbare Zwecke arbeitete, in die Zentralstelle für die Sicherheit in der Informationstechnik (ZSI) erweisen. Sie soll als Bundesoberbehörde mit der Bezeichnung „Bundesamt für Sicherheit in der Informationstechnik (BSI)" im Geschäftsbereich des Bundesministers des Innern eingerichtet werden und unabhängig vom Aufgabenbereich Sicherheitsrisiken bei der Anwendung der Informationstechnik untersuchen, Maßnahmen zur Gewährleistung der Sicherheit entwickeln, Kriterien für die Prüfung und Bewertung von Systemen und Komponenten der Informationstechnik erarbeiten und auf der Basis dieser Kriterien für angebotene Systeme und Komponenten Sicherheitszertifikate vergeben. Daneben soll sie insbesondere allgemein in Sicherheitsfragen beraten und die zuständigen Stellen bei der Bekämpfung krimineller Aktivitäten gegen die Sicherheit bei der Anwendung der Informationstechnik unterstützen. Auf meine Forderung hin soll vorgesehen werden, daß sie auch meine Arbeit im Bereich Datensicherung unterstützt, wobei meine Unabhängigkeit gewahrt bleiben muß.

Ich begrüße, daß dieses Konzept die Billigung des Bundeskabinetts gefunden hat, weil damit deutlich gemacht wird, daß die Sicherheit der Datenverarbeitung nicht auf Anwendungen in einigen Bereichen beschränkt bleiben darf, insbesondere keine Aufgabe nur für den Bereich der Geheimdienste ist. Das Konzept macht klar, daß Sicherheit Bestandteil jeder Datenverarbeitung sein muß. Denn nur eine gut organisierte und sichere Datenverarbeitung setzt den Betreiber in die Lage, seine Datenverarbeitung zu beherrschen, also vor allem ihre Rechtmäßigkeit garantieren zu können. Ich hoffe, daß der bereits erfolgten Umbenennung der erwähnten Zentralstelle bald die gesetzliche Zuweisung der neuen Aufgaben folgt.

Bereits unter dem neuen Namen hat die ZSI „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (GMBl 1989, S. 278f.) herausgegeben. Damit wurden zum einen Funktionsklassen für Sicherheitsmaßnahmen und zum anderen Abstufungen der Qualität der Datensicherheit definiert. Dieser Katalog soll die Grundlage für Zertifizierungen bilden und wird auch als deutscher Beitrag in die entsprechenden europäischen Diskussionen eingebracht. Weitere Arbeiten werden folgen und für Hersteller und Anwender von DV-Systemen die notwendigen Orientierungshilfen bieten. Es wird jedoch voraussichtlich noch einige Jahre dauern, bis diese in die Zukunft gerichteten Maßnahmen in der Praxis der Datenverarbeitung der (öffentlichen und der privaten) Anwender im notwendigen Umfang wirken.

Schneller wirksam könnte das ebenfalls vom ISIT beratene und vom Kabinett gebilligte „Rahmenkonzept zur Gewährleistung der Sicherheit bei Anwendung der Informationstechnik -IT-Sicherheitsrahmenkonzept" werden, das Hilfen für die von den einzelnen Dienststellen in ihrem IT-Rahmenkonzept darzustellenden Sicherheitskonzepte enthält. Zum Erfolg sind aber in erster Linie Anstrengungen in den Stellen selbst nötig, die durch derartige Hilfen nur unterstützt und auch durch die besten Rahmenkonzepte nicht ersetzt werden können. Deshalb ist es besonders zu bedauern, daß nach einer vom Bundesminister des Innern vorgenommenen Zusammenstellung der Aus- und Fortbildungskonzepte der Ressorts für die insgesamt 30 000 in der Informationstechnik zu schulenden Mitarbeiter im Durchschnitt nur knapp DM 150 pro Mitarbeiter und Jahr an Schulungsaufwand eingeplant sind. Dieser Rahmen ist so eng, daß der Anteil, der davon auf Schulung in Fragen der Datensicherheit entfallen wird, kaum eine Gewähr für die notwendige rasche und durchgreifende Verbesserung der Situation bietet.

24.2 Arbeitsplatzcomputer

In dem vom Bundesministerium des Innern herausgegebenen IT-Bestandsverzeichnis (Stand: 31. Dezember 1988) sind 15 225 gemeldete Datenverarbeitungssysteme ausgewiesen. Davon sind 10 741 Einplatzsysteme. Das macht deutlich, daß die Zahl der Arbeitsplatzcomputer (APC) in der Bundesverwaltung in den letzten Jahren deutlich gestiegen ist. Unter der Bezeichnung Arbeitsplatzcomputer sind unterschiedliche Geräte im Einsatz. Bei der Mehrzahl handelt es sich um IBM-kompatible Personalcomputer (PC) mit dem Betriebssystem MS-DOS. Daneben werden ähnlich leistungsfähige Geräte anderer Art eingesetzt. Es sind aber auch Homecomputer anzutreffen und in neuester Zeit brieftaschengroße Datenbankrechner. Inzwischen findet man aber auch schon genauso kleine Personalcomputer mit dem Betriebssystem MS-DOS. Ein Teil dieser kleinen Computer hat eine Schnittstelle, die eine Verbindung mit anderen Rechnern möglich macht. Damit setzt sich die Tendenz zur Miniaturisierung und zur Preissenkung für DV-Leistung fort. Leider halten die Datenschutz- und Datensicherungsmaßnahmen mit dieser Entwicklung nicht Schritt.

24.2.1 Ergebnis einer Umfrage

Nachdem mir durch Kontrollen bekannt geworden war, daß es beim Einsatz von Personalcomputern sehr häufig zu erheblichen datenschutzrechtlichen Mängeln kommt (siehe auch meinen 11. TB S. 85 ff.), habe ich eine Umfrage bei den obersten Bundesbehörden durchgeführt, um mir einen Überblick über die Maßnahmen zur Organisation und Eigenkontrolle in diesem Bereich zu verschaffen. Dabei wurden folgende Fragen gestellt:

1. Welche besonders auf die Anwendung von APC eingehenden Vorschriften bestehen für ihren Geschäftsbereich oder einzelne Dienststellen im Geschäftsbereich?

2. Welche Maßnahmen sind besonders darauf gerichtet, die Anwender von APC mit den Datenschutzvorschriften vertraut zu machen?

3. Für welche Stellen im Geschäftsbereich gibt es ein Verzeichnis *sämtlicher* DV-Anlagen oder *sämtlicher* Arbeitsplatzcomputer? Wenn ja, welche Angaben über die einzelnen Anlagen sind darin enthalten und mit welchen Mitteln wird die Vollständigkeit des Verzeichnisses angestrebt?

4. Welche Vorschriften regeln den Einsatz, die Beschaffung oder die Erstellung von Programmen insbesondere für APC?

5. Welche Vorschriften (Verbote, Meldepflichten, Genehmigungsvorbehalte o.ä.) regeln die Verwendung privater Homecomputer, PC und anderer privater, an DV-Anlagen anschließbarer Geräte (z. B. Drucker oder Speichereinheiten) sowie privater Datenträger?

6. Welche Maßnahmen werden durchgeführt, um die tatsächlich stattfindende Nutzung von APC und die Art der dabei tatsächlich verarbeiteten Daten festzustellen und zu kontrollieren?

Nach Auswertung der Antworten ergibt sich ein recht unterschiedliches Bild.

Vorschriften, die den Einsatz von APC regeln, sind bei einem Teil der befragten Stellen erst in Vorbereitung, bei anderen sind sie in sehr detaillierter Form bereits seit längerem vorhanden. Dies ist offenkundig auf den unterschiedlichen Zeitpunkt des Beginns des APC-Einsatzes zurückzuführen.

Ähnliches gilt für Regelungen über Maßnahmen, die die APC-Benutzer mit Datenschutzvorschriften vertraut machen sollen. Neben der Verpflichtung gemäß § 5 BDSG werden häufig eine besondere Schulung, aber auch die Aufnahme von entsprechendem Lehrstoff in die allgemeine Ausbildung erwähnt. Bei einer Reihe von Stellen wird auch die ständige Beratung durch den internen Datenschutzbeauftragten genannt, aber auch die Teilnahme der APC-Benutzer an externen Seminaren.

Ein Verzeichnis der DV-Anlagen einschließlich der APC wird nach den eingegangenen Antworten bei allen Stellen geführt.

An Vorschriften zum Einsatz, für die Beschaffung oder Erstellung von Software werden häufig die „Besonderen Vertragsbedingungen" für DV-Leistungen der KBSt und die „Richtlinien für den Einsatz der Informationstechnik in der Bundesverwaltung (IT-Richtlinien)" genannt, ein Teil der Behörden antwortet jedoch auch, das sei noch nicht geregelt.

Die Verwendung privater Homecomputer, APC und sonstiger privater Hardware ist bei der weit überwiegenden Mehrheit der befragten Stellen verboten. Dieser Anteil steigt, wie ich aus Rückfragen erfahren habe.

Die Kontrolle des Einsatzes und der Verwendung der APC ist anscheinend nach wie vor ein Problem. In den Antworten der befragten Stellen wird zum Teil auf diese Frage nicht eingegangen, zu einem anderen Teil ist die Antwort vage („im Rahmen der üblichen Dienstaufsicht"). Ein Teil der Behörden räumt ein, es gebe dazu noch keine Regelung. Einige der Stellen geben jedoch auch an, es werde eine regelmäßige Kontrolle durchgeführt.

Eine Gesamtbewertung ist schwierig, weil die Regelungen jeweils im Zusammenhang mit Art und Umfang des APC-Einsatzes beurteilt werden müssen. Bei aller Unterschiedlichkeit fällt auf, daß doch recht häufig auf allgemein für die Datenverarbeitung geltende Vorschriften verwiesen wird, die sich nach meinen Erfahrungen als wenig geeignet und überwiegend unzureichend erwiesen haben. Eine Ausnahme davon bildet allein das weit verbreitete Verbot privater Geräte, womit — wenn es konsequent durchgesetzt wird — wenigstens einem der Risiken wirksam zu begegnen ist.

Auffallend wenig detailliert sind die Vorschriften zur Kontrolle der APC-Nutzung durch die Dienststellen selbst. Daß hier ein wesentliches Defizit liegt, bestätigte sich auch in den von mir durchgeführten Kontrollen: Bisher habe ich noch keine einzige Behörde ange-

troffen, in der APC von der Behörde selbst oder einer Fachaufsicht tatsächlich kontrolliert wurden. Das hatte zur Folge, daß es in vielen APC Dateien mit personenbezogenem Inhalt gab, von deren Existenz weder der interne Datenschutzbeauftragte noch die Dienststellenleitung wußte.

Ähnliches gilt für die verwendete Software. So sind oft auch nicht dienstlich beschaffte Programme vorhanden, bei denen zudem manchmal sogar der Bezug zur Aufgabenerfüllung fehlt. Unter diesen Umständen kann die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, deren Überwachung in § 15 BDSG ausdrücklich verlangt wird, nicht gewährleistet werden.

24.2.2 Ergebnisse aus Prüfungen

Weil mir die Schwierigkeiten beim Einsatz von APC bei der Deutschen Bundespost bekannt waren (s. 11. TB S. 35), habe ich auch im Berichtsjahr dort den Einsatz von APC kontrolliert. Dabei habe ich festgestellt, daß die Praxis noch immer nicht der Weisungslage entsprach. Noch immer gab es Dateien, die nicht zu dem bei mir geführten Register gemäß § 19 Abs. 4 BDSG gemeldet waren. Darüber hinaus habe ich in einem Fall den Einsatz eines privaten PC festgestellt. Mit einem Rechner wurden Dienst- und Einsatzpläne erstellt. Auch die dafür genutzten Dateien waren nicht zum Register gemeldet. Eine Beteiligung des Personalrates nach § 75 Abs. 3 Nr. 17 BPersVG hatte nicht stattgefunden.

Der BMPT hat mir daraufhin mitgeteilt, ein Teil der nicht gemeldeten Dateien sei gelöscht worden; die anderen wurden nachträglich zum Register gemeldet. Die Nutzung privateigener PC für dienstliche Zwecke wurde für unzulässig erklärt, der bei meiner Kontrolle vorgefundene private PC aus den Diensträumen entfernt. Die Amtsleitung des geprüften Amtes hat den betreffenden Personalrat erneut über die automatisiert erstellten Dienstpläne informiert. Dieser hat keine Einwände erhoben.

Der BMPT hat alle Behörden der Bundespost noch einmal auf das Verbot einer individuellen Datenverarbeitung außerhalb von genehmigten DV-Anwendungen hingewiesen. Diese hatte nämlich dazu geführt, daß Dateien entstanden, aber nicht zum Register gemeldet worden waren.

Der BMPT hat darüber hinaus „Merkblätter für Einzelplatzsysteme" entwickelt und ist darum bemüht, die dort getroffenen Regelungen in die Praxis umzusetzen. Wo sensible Daten verarbeitet werden, soll künftig Sicherheitsoftware eingesetzt werden. Weitere Beratungsgespräche mit mir wurden vereinbart.

Auch in den Bundesministerien gibt es eine große Anzahl von Arbeitsplatzcomputern. Um mir ein Bild von den hier durchgeführten Datenschutz- und Datensicherungsmaßnahmen zu machen, habe ich den APC-Einsatz in einem Ministerium gemäß § 19 Abs. 1 BDSG kontrolliert.

Vor dem Beginn einer Kontrolle des APC-Einsatzes im Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit war mir mitgeteilt worden, es seien *sechzehn* Personalcomputer vorhanden.

Im Laufe der Kontrolle wurde festgestellt, daß in diesem Ministerium außer *neunzehn* dienstlich beschafften APC noch je ein APC einer nicht zum Ressort gehörenden Körperschaft und des Telefonanlagenherstellers, der die Nebenstellenanlage betreut, sowie eine unbekannte Anzahl privater PC betrieben wurden.

Zwölf der dienstlich beschafften APC arbeiten in einem zentral gesteuerten Netz. Sie haben kein Diskettenlaufwerk, sind mit einer Sicherheitssoftware in das System eingebunden und mit mobiler Festplatte ausgestattet.

Diese APC werden überwiegend in Emulation als Terminals des zentralen Systems genutzt. Ihre Einbindung ist angemessen gesichert. Der Benutzer hat nur Zugriff auf die Arbeitsmittel, die er für seine Aufgabenerfüllung benötigt. Er kann keine eigenen Verfahren entwickeln und Dateien einrichten, da er nicht über eine freie Kommandosprache verfügt, sondern nur über compilierte Programme. Dieses Konzept habe ich aus datenschutzrechtlicher Sicht ausdrücklich begrüßt.

Ganz anders waren die Verhältnisse beim APC-Einsatz außerhalb des vernetzten Systems. Dort waren auf den Festplatten einiger der Geräte Programme vorhanden, die für die Aufgabenerfüllung nicht erforderlich waren. Sicherheitssoftware wurde nicht verwendet.

Gleichwohl wurden dort zum Teil personenbezogene Daten verarbeitet. Eine Einbindung ins Netz des Ressorts erscheint mir daher dringend geboten. Sollte dies in Einzelfällen nicht möglich sein, ist bei Verarbeitung personenbezogener Daten jedenfalls die gleiche Sicherheit herzustellen, die bei den vernetzten APC besteht.

Der Einsatz von nicht ressort-eigenen APC ist problematisch; insbesondere gilt dies für die Verarbeitung von Daten über Mitarbeiter des BMU in dem APC der Firma, die die Nebenstellenanlage wartet. Das Ressort ist für die Daten seiner Mitarbeiter verantwortlich. Die Verfügungsgewalt über das Gerät, die Daten und die Programme zu ihrer Verarbeitung lag jedoch allein bei der Firma. Dies ist datenschutzrechtlich nicht vertretbar. Ebenso ist es nicht vertretbar, daß andere Datenverarbeitungsanlagen, die sich nicht im Eigentum des Ressorts befinden, dort für die Aufgabenerfüllung verwendet werden, ohne daß durch konkrete Vereinbarung die Verfügung über die Daten und die Ergebnisse der Datenverarbeitung für das Ressort gesichert ist. Auch fehlt die gebotene Kontrolle. Eine solche Kontrolle hätte verhindern müssen, daß in diesen APC Programme vorgehalten werden, die offensichtlich ohne Freigabe und zumindest zum Teil auch ohne dienstliches Bedürfnis eingebracht wurden.

Ich habe diesen ungeregelten und unkontrollierten Einsatz von APC beanstandet. Begrüßt habe ich die während der Kontrolle betonte Absicht, den Einsatz privater Rechner zu untersagen. Für die Erstellung einer Hausanordnung habe ich meine Beratung angeboten. Der BMU hat inzwischen nahezu alle Bean-

standungen anerkannt und die Beseitigung der angesprochenen Mängel zugesagt.

Die Ergebnisse aus diesen Kontrollen geben erneut Anlaß, darauf hinzuweisen, daß APC mit dem Betriebssystem MS-DOS ohne zusätzliche Sicherheitssoftware für die Verarbeitung sensibler personenbezogener Daten nicht geeignet sind, weil angemessene Maßnahmen im Sinne des § 6 BDSG nicht getroffen werden können.

Wenn keine zusätzliche Sicherheitssoftware eingesetzt wird, ist es auch praktisch unmöglich, die Benutzung von nicht dienstlich freigegebenen Programmen zu verhindern. Fehlen dann sowohl Kontrollen als auch eingehende und wirksame Belehrungen der Benutzer, dann ist es nicht verwunderlich, daß selbsterstellte oder privat erworbene Programme eingesetzt werden. Das können — und in einigen der kontrollierten Fälle lag diese Vermutung sehr nahe — dann auch „Raubkopien" oder sonst von unklaren Quellen bezogene Programme sein. Abgesehen davon, daß bei einem solchen Verfahren die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme nicht gewährleistet ist, können mit so beschafften Programmen auch Viren eingeschleppt und andere Störungen der Verfügbarkeit von Geräten, Daten und Programmen verursacht werden. Die Gefährdungen sind also keineswegs auf Verstöße gegen Vorschriften zum Schutz personenbezogener Daten beschränkt.

24.2.3 Empfehlungen für die Praxis

Ein wesentlicher Grund für die praktischen Mängel beim Einsatz von APC dürfte darin liegen, daß den Verantwortlichen in den einzelnen Dienststellen häufig die tatsächliche Situation in ihrer Dienststelle nicht bekannt ist. Deshalb wird der Organisationsbedarf nicht erkannt, und Weisungen bleiben ebenso ohne praktische Auswirkungen wie z. B. die von der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung (KBSt) veröffentlichten „Unterlagen für den Einsatz von Arbeitsplatzrechnern in der Bundesverwaltung" (Band 7 der Schriftenreihe der KBSt) oder andere gute Hilfen.

Auch vom typischen PC-Praktiker selbst sind von allein kaum Bemühungen um mehr Sicherheit und insbesondere mehr Kontrollierbarkeit zu erwarten. Es handelt sich in der Regel um hochmotivierte und aktive Mitarbeiter, die entsprechend stark mit Arbeit belastet sind, und die überzeugt sind, ihre eigenen Organisationsprobleme gelöst zu haben.

Um trotzdem praktische Verbesserungen zu erreichen, habe ich in einem Rundschreiben an die obersten Bundesbehörden empfohlen, daß in jeder Dienststelle ein Verzeichnis der tatsächlich eingesetzten APC und der dabei verwendeten Datenträger geführt wird. Grundlage dieser Verzeichnisse sollen die einfach auszufüllenden Formblätter sein, die als Anlage 11 diesem Bericht beigefügt sind. Auf diesen von mir aufgrund einer Untersuchung im Bundesverwaltungsamt und mit der praktischen Unterstützung durch die Bundesstelle für Büroorganisation und Bürotechnik so entwickelten Formblättern können die tatsächlichen Verhältnisse mit möglichst wenig Aufwand so dargestellt werden, daß daraus ein bestehender weiterer Handlungsbedarf zu erkennen ist.

24.2.4 Sicherheitssoftware für PC

In meinem Elften Tätigkeitsbericht (S. 84) hatte ich darauf hingewiesen, daß sich die technischen Möglichkeiten zur Unterstützung von PC-Sicherheit deutlich verbessert haben. Dieser Trend hat sich fortgesetzt: Eine Vielzahl von Produkten aus dem In- und Ausland werden angeboten. Für den PC-Benutzer ist es oft schwierig, dieses breite Angebot zu überschauen. Inzwischen stehen aber Marktübersichten und Testberichte zur Verfügung, an denen man sich orientieren kann. Besonders hinzuweisen ist auf das kostenlos abgegebene „Angebotsverzeichnis PC-Sicherheitssoftware" (4. Auflage) der Gesellschaft für Datenschutz und Datensicherung GDD. Es enthält Herstellerangaben u. a. zu Preis, Leistungsumfang und Zahl der Installationen. Eine fünfte Auflage soll 1990 erscheinen. Nach meinem Eindruck ist gegenwärtig etwa ein halbes Dutzend ausgereifter Produkte auf dem Markt, mit denen die Anforderungen des § 6 BDSG erfüllt werden können. Mehrere Hersteller haben bei der ZSI Zertifikate für ihre Software beantragt; erteilt wurde nach meiner Kenntnis erst ein Zertifikat, ein weiteres Produkt wird zur Zeit geprüft.

Leider werden die vorhandenen Möglichkeiten zu selten genutzt. Die weit überwiegende Zahl der APC, mit denen personenbezogene Daten verarbeitet werden, ist, sieht man einmal von einem Schlüsselschalter ab, völlig ungeschützt. Es zeigt sich aber in der Praxis immer wieder, daß Gefährdungen gegeben sind; es wurden z. B. mehrfach PC mit sensiblen Daten auf der Festplatte gestohlen. Es ist anzunehmen, daß es den Tätern dabei weniger um die Daten als vielmehr um das Gerät ging; es ist aber nicht auszuschließen, daß Daten, deren Wert ein Täter erkennt, auch verkauft oder auf andere Weise mißbräuchlich verwendet werden. Deshalb ist die Sicherheitslage noch einmal darzustellen:

Daten auf der Festplatte eines PC mit dem Betriebssystem MS-DOS sind jedermann, der Zugang zu dem Rechner hat, frei zugänglich. Deshalb müssen auf jeden Fall die Räume gesichert werden. Ein Schlüsselschalter am PC ist sinnvoll, weil damit bei vorübergehender Abwesenheit die Benutzung durch Unbefugte erheblich erschwert werden kann. Sein Wert darf aber nicht zu hoch eingeschätzt werden, da er — wenn man genügend Zeit dafür aufwenden kann — auch überbrückt werden kann. Werden Daten mit einiger Aussagefähigkeit verarbeitet, ist der Einsatz einer Sicherheitssoftware unverzichtbar. Sie sollte mindestens folgendes leisten:

— Benutzeridentifizierung und -authentifizierung,

— sichere Menüführung, die einen Zugang zum Betriebssystem verhindert oder restriktiv regelt (auf den Zugang nur zu eigenen Daten und nur mit bestimmten Kommandos),

— wirkliches Löschen von Dateien (durch Überschreiben),

— sichere kryptografische Verschlüsselung aller Daten auf der Festplatte, den Disketten und — soweit vorhanden — den Magnetbändern,

— Protokollierung der Benutzeraktivitäten.

Der Einsatz einer Sicherheitssoftware bedingt, daß es neben dem Benutzer auch einen Systemverwalter gibt, der die Implementierung vornimmt und den Benutzern ihre Rechte zuordnet (Benutzerprofil). Die angebotene Sicherheitssoftware sollte auch hinsichtlich ihrer Benutzerfreundlichkeit ausgewählt werden. Der Benutzer selbst sollte möglichst wenig von ihrem Vorhandensein merken, und für den Systemverwalter sollte sie bequem handhabbar sein. Nur dann, wenn die Software leicht zu handhaben ist, werden bei der Implementierung voraussichtlich auch alle Sicherheitskomponenten aktiviert; die Benutzeroberfläche für den Systemverwalter ist also nur scheinbar Nebensache. Die Aktivitäten des Systemverwalters sollten nachvollziehbar sein. Manche Produkte bieten daher eine Revisionsfunktion an. Einige Produkte sehen auch vor, daß die Funktionen der Systemverwaltung stets von zwei Personen im Zusammenwirken ausgeführt werden (Vieraugenprinzip).

24.2.5 Personaldaten auf Arbeitsplatzcomputern

Bereits in meinem Sechsten (S. 18 f.) und Siebenten Tätigkeitsbericht (S. 19) habe ich von der Entwicklung eines Personalinformationssystem bei einer obersten Bundesbehörde berichtet. Damals war die Realisierung des Vorhabens auf einem Großrechnersystem vorgesehen. Die Benutzung von Arbeitsplatzcomputern (APC) kam nicht infrage, weil sich damit die Anforderungen der Anlage zu § 6 BDSG nicht erfüllen ließen. Im Berichtszeitraum bat diese oberste Bundesbehörde um eine Beratung, da nunmehr geplant war, das Verfahren mit einem APC zu realisieren, und zwar mit einem Rechner mit austauschbarer Festplatte und dem Betriebssystem MS-DOS. Das Personalinformationssystem sollte mit einem Datenbanksystem entwickelt und die einzelnen Programme compiliert werden; dem Benutzer sollte also keine freie Abfrage zur Verfügung stehen. Um die Erfüllung der Anforderungen des § 6 BDSG zu ermöglichen (s. 8. TB S. 17f., S. 56ff.), sollte das Gerät ferner mit einer Sicherheitssoftware ausgestattet werden. Nach einer grundsätzlichen Beratung über die notwendigen Sicherungsmaßnahmen wurde das System entwickelt und mir anschließend vorgestellt. Dabei ergaben sich im Vergleich zu den in meinem Achten Tätigkeitsbericht beschriebenen Kriterien einige Probleme, für die sich angemessene Lösungen finden ließen:

— Die Sicherheitssoftware bietet zwar die Möglichkeit, Mindestanforderungen für das Paßwort des Benutzers zu setzen (Länge, Zusammensetzung, Wechsel). Diese Kriterien gelten jedoch nicht für das Paßwort des Systemverwalters. Dessen Benutzername war überdies „System", was leicht zu erraten war. Dieser Name wurde geändert und für die Wahl des Paßwortes wurden besondere Regeln festgelegt.

— Die strikte Menüführung war noch nicht gewährleistet, da es sowohl vom Personalinformationssystem als auch vom Textverarbeitungssystem Zugang zum Betriebssystem gab. Der Zugang zum Betriebssystem wird (ggf. mit einer neuen Version der Sicherheitssoftware) abgestellt.

— Das elektronische Bauteil zum Verhindern des Ladens eines anderen Betriebssystems über das Diskettenlaufwerk paßte nicht zum Rechner. Das Disketten-Laufwerk wird zunächst, bis ein passendes Bauteil für diese wichtige Sicherheitsfunktion zur Verfügung steht, völlig außer Betrieb gesetzt. Das Gehäuse wird dann versiegelt.

— Es erfolgt keine kryptografische Verschlüsselung. Auf eine kryptografische Verschlüsselung wird angesichts der Aufbewahrung der Platte im Safe und der Tatsache, daß der Rechner (nur offline) in dem abgeschlossenen Bereich der Personalabteilung von nur vier Benutzern betrieben wird, verzichtet.

— Im System werden drei Dokumentations-Dateien geführt, die zur Verhaltens- und Leistungskontrolle geeignet sind, die aber nach einer Vereinbarung zwischen der Behörde und dem Personalrat aus dem Jahre 1987 unzulässig ist. Deshalb wurde festgelegt, daß die Dokumentationsdateien nur für Zwecke des Datenschutzes und der Datensicherung genutzt werden und daß darauf nur der interne Datenschutzbeauftragte und der Systemverwalter gemeinsam zugreifen dürfen.

Die Beteiligung an diesem Projekt war zwar recht personalintensiv; es zeigte sich jedoch erneut, daß mein Beratungsauftrag dann sinnvoll realisiert werden kann, wenn meine Beteiligung in einem frühen Entwicklungsstadium erfolgt, weil dann Datenschutzaspekte noch ohne großen Aufwand in die Entwicklung einfließen können.

24.3 Verbindungsdatenspeicherung in internen Telefonanlagen

Unter Nr. 7.2.1 habe ich auf Probleme aufmerksam gemacht, die sich insbesondere im neuen ISDN-Telefonnetz der DBP aus der Digitalisierung der Verbindungssteuerung und der Speicherung der Verbindungsdaten ergeben. Schon seit einigen Jahren sind in Behörden und Unternehmen interne Telefonanlagen — früher Telefonnebenstellenanlagen, künftig Telekommunikationsanlagen (TK-Anlage) genannt — in Betrieb, in denen in großem Umfang Verbindungsdaten registriert und weiterverarbeitet werden. Ein nennenswerter Anteil dieser Anlagen ist bereits „ISDNfähig" ausgerüstet, so daß diese Anlagen grundsätzlich sofort dann mit dem öffentlichen ISDN-Netz verbunden werden können, wenn der regionale Netzausbau der DBP dies zuläßt.

Wie in den Ortsvermittlungsstellen der Deutschen Bundespost wird auch in den TK-Anlagen für jedes Telefongespräch ein vollständiger Verbindungsdatensatz erzeugt, der u. a. genaue Angaben über Zeitpunkt, Dauer und Gebühreneinheiten sowie die gewählte Telefonnummer enthält. Diese Daten können über das Verbindungsende hinaus gespeichert und weiter verarbeitet werden. So kann nicht nur die im

Verlauf eines Gesprächs entstandene Gebühr errechnet werden; es können vielmehr auch Ausdrucke gemacht werden, die Auflistungen aller geführten Gespräche für einen bestimmten Zeitraum enthalten, geordnet nach Telefonnummern und/oder Organisationseinheiten.

Neben den Verbindungsdaten werden jedoch — unabhängig von tatsächlich geführten Telefonaten — für jeden Anschluß administrative Daten gespeichert, die den „Bestandsdaten" im Telefondienst der DBP (§ 449 TKO) vergleichbar, meistens jedoch sehr viel umfangreicher sind: Name des Anschlußinhabers, Art der Berechtigung (Ortsgespräche, Ferngespräche usw.), Kurzwahlziele des Anschlußinhabers (oft gewählte private und dienstliche Telefonnummern), Geheimnummer des elektronischen Telefonschlosses usw. Diese sowie die Verbindungsdaten sind in der Regel Daten über Beschäftigte der Stelle und geeignet, zur Kontrolle von deren Verhalten und Leistung verwendet zu werden (siehe auch oben Nr.6.3).

Eine andere Problematik ergibt sich daraus, daß für Bedienstete der Liefer- oder Servicefirma — im Rahmen der Betreuung der Anlage — grundsätzlich die Möglichkeit besteht, die in der Anlage gespeicherten Daten einzusehen oder sogar zu kopieren. Dies gilt für Tätigkeiten im Rahmen der Wartung oder auch der Softwarepflege, die bislang überwiegend vor Ort von einem Techniker vorgenommen werden. Dabei ist keineswegs immer von mißbräuchlichem Handeln auszugehen: Hat der Betreiber der TK-Anlage die Verbindungsdaten nicht gegen Zugriff geschützt, können sie z. B. im Rahmen einer Wartung dem Techniker angezeigt oder ausgedruckt werden, was gelegentlich die Fehlersuche erleichtern kann.

In zunehmenden Maße — auch wegen der geringeren Kosten — vereinbaren die Anlagenbetreiber eine sogenannte Fernbetreuung oder -wartung. Zu diesem Zweck ist die TK-Anlage über Leitungen der DBP mit dem Fernbetreuungszentrum — einer Rechenanlage — der Betreuungsfirma verbunden. Dabei können nicht nur viele Fehler behoben werden, die von der TK-Anlage dem Rechner der Betreuungsfirma automatisch gemeldet werden, auch eine erforderliche Reparatur vor Ort wird wesentlich erleichtert, wenn der Techniker aufgrund der Fehlermeldung bereits die auszutauschende Baugruppe zum Kunden mitnehmen kann. Schließlich können der TK-Anlage auch neue Softwaremodule übermittelt werden, sei es zur Softwarepflege, sei es, weil der Betreiber vertraglich zusätzliche Leistungsmerkmale vereinbart hat.

Über die Speicherung und Verarbeitung von Verbindungs- und administrativen Daten in digitalen TK-Anlagen habe ich mit zwei führenden Herstellern intensive Gespräche geführt. Die Ergebnisse lassen sich in folgenden Empfehlungen für die Beschaffung und den Betrieb solcher Anlagen zusammenfassen:

a) Art und Inhalt der Dateien

Die mit den Verhandlungen beauftragten Mitarbeiter der Lieferfirma gehören in der Regel der Vertriebsorganisation des Unternehmens an. Sie sind daher sehr häufig nicht oder nicht vollständig darüber informiert, welche Dateien mit personenbezogenen (d. h. anschlußbezogenen) Daten vom System automatisch erzeugt werden und welche Daten sie im einzelnen enthalten. Diese Kenntnisse sind jedoch für die betreibende Behörde als datenschutzrechtlich verantwortliche Stelle unerläßlich. Auf entsprechenden Erläuterungen, auch durch Experten, sollte bestanden werden.

b) Schutz der Dateien

TK-Anlagen verfügen über ein Betriebsterminal — i.d.R. mit Drucker —, auf dessen Bildschirm für Administrations- und Wartungszwecke Dateieninhalte angezeigt werden. Auch für dieses Terminal gelten die Forderungen aus der Anlage zu § 6 BDSG. Es ist daher durch geeignete Vorkehrungen sicherzustellen, daß das Terminal nur von Befugten benutzt werden kann (z. B. durch Verwendung von Schlüsselschaltern oder entsprechende Raumsicherung) und daß nur Befugte die einzelnen Dateien im Rahmen ihrer Aufgabenstellung einsehen und auswerten können. Letzteres erfordert einen gestaffelten Paßwortschutz, der jedem Berechtigten nur den Zugriff zu den vom Systemverwalter festgelegten Bereichen erlaubt. Das Paßwort für Behördenexterne (Wartungstechniker usw.) darf grundsätzlich keinen Zugriff auf personenbezogene Daten der Behörde erlauben und ist von der betreibenden Behörde festzulegen. Abzulehnen sind Lösungen, bei denen ein vom Hersteller festgelegtes Paßwort den Zugriff auf Daten, Programme und Funktionen schützt, das „nur" der Kundendienstorganisation dieses Herstellers (z. B. einheitlich für Europa) bekannt ist. Solche Paßwörter können aus organisatorischen Gründen über lange Zeit nicht gewechselt werden, überdauern deshalb das Ausscheiden von Mitarbeitern und können leicht bekannt werden.

Sofern das Betriebsterminal Hardcopy-Ausdrucke ermöglicht, deren Anfertigung vom System nicht protokolliert wird, sollten das Druckerpapier fortlaufend numeriert und der Verbleib der Ausdrucke dokumentiert werden.

c) Unterdrückung einzelner Verbindungsdaten

In den TK-Anlagen werden die Verbindungsdaten der Telefonate in der Regel sehr detailliert gespeichert, sie enthalten z. B. häufig den sekundengenauen Zeitpunkt von Beginn und Ende des Telefonates sowie die volle Rufnummer des Angerufenen. Für die Speicherung und Verarbeitung von Verbindungsdaten in TK-Anlagen bestehen jedoch in der Regel Dienstvereinbarungen zwischen dem Dienstherrn und dem Personalrat der Behörde, in denen auch der Umfang der zu speichernden Verbindungsdaten geregelt ist. Auch gelten für die Benutzung der Telefonanlagen in den Bundesbehörden die „Dienstanschlußvorschriften" des Bundesministers der Finanzen (vgl. 11. TB S. 26 f.). Oft wird eine derart detaillierte Verbindungsdatenerfassung, wie sie die Technik der TK-Anlagen ermöglicht, nach diesen Regelwerken nicht zulässig sein. So sieht die demnächst in Kraft tretende Neufassung der Dienstanschlußvorschriften die Erfassung der Uhrzeit der Telefonate nicht vor und verlangt bei Privatgesprächen eine Kürzung der angewählten Telefonnummer um die letzten beiden Stellen. Vorliegende

Erfahrungen lassen es erforderlich erscheinen, sich vom Auftragnehmer die Einhaltung dieser Forderungen ausdrücklich zusichern zu lassen. Wenn die entsprechenden Festlegungen bis zum Vertragsschluß nicht erfolgt sind, sollte vertraglich geregelt werden, zu welchen Bedingungen (Kosten, Fristen) und in welchem Umfang die noch zu treffenden Festlegungen technisch realisiert werden.

d) Verbindung zum Fernbetreuungszentrum

Die Verbindung von der TK-Anlage zum Fernbetreuungszentrum erfolgt über Wählleitungen der Deutschen Bundespost. Gebräuchlich ist dabei die Verwendung des Telefonnetzes — unter Verwendung eines Modems — oder aber des DATEX-Netzes. In beiden Fällen handelt es sich um ein offenes Wählnetz, das grundsätzlich die Möglichkeit bietet, daß ein Unbefugter („Hacker") den Fernbetreuungsanschluß der TK-Anlage anwählt, um die gespeicherten Daten einzusehen oder die Software zu beschädigen. Die Behörde sollte sich deshalb darlegen lassen, welche Sicherungsvorkehrungen die Lieferfirma zur Verhinderung solcher Zugriffe vorgesehen hat. Zweckmäßig ist z. B. die Einrichtung eines automatischen Rückrufes: Wird die TK-Anlage „angerufen", wird nicht sofort eine Verbindung zum Anrufer hergestellt, sondern zunächst die Verbindung beendet, danach die Anschlußnummer des Fernbetreuungszentrums angerufen und erst damit die Verbindung zu diesem hergestellt. Eine Alternative besteht darin, den Modem (manuell) abzuschalten, so daß ein Verbindungsaufbau erst nach erneuter Schalterbetätigung — durch die Behörde — möglich ist.

e) Auslagerung sensibler Programme

Auch wenn technisch weitgehend sichergestellt werden kann, daß nur Berechtigte — vor Ort oder über Leitungen — Zugang zur TK-Anlage erhalten, muß doch sichergestellt werden, daß deren Zugriffe auch im Einzelfall nur im Rahmen des Zulässigen bleiben. Läßt sich dies durch einen Paßwortschutz erreichen, so kann es erforderlich sein, das Paßwort für den speziellen Technikerzugang seitens der Behörde geheimzuhalten, es dem Techniker nur im Einzelfall bekanntzugeben und danach sofort ändern. Häufig ist es auch zweckmäßig, statt dessen die „gefährlichen" Software-Komponenten — z. B. diejenigen, die ein Kopieren der gespeicherten Dateien ermöglichen — nicht ständig verfügbar zu halten, sondern erst im Bedarfsfalle über Diskette zu laden und hinterher wieder zu löschen. Auch hierfür sollte die Behörde ein schlüssiges Konzept verlangen.

25 Entwicklung des allgemeinen Datenschutzrechts

In meinem Elften Tätigkeitsbericht (S. 85ff.) habe ich über den von der Bundesregierung eingebrachten Entwurf eines Artikelgesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes berichtet und dabei insbesondere auf die zum Teil konzeptionellen Mängel des darin enthaltenen Entwurfs einer Neufassung des Bundesdatenschutzgesetzes hingewiesen. Der Bundesrat hat in seiner insgesamt 69 Punkte umfassenden Stellungnahme zu diesem Teil des Gesetzentwurfs und der damit verbundenen Ergänzung des Verwaltungsverfahrensgesetzes ebenfalls eine überwiegend kritische Position bezogen. Seine Stellungnahme deckt sich oft mit der von mir vertretenen Meinung. Die Bundesregierung hat in ihrer Gegenäußerung nur einem Teil der Vorschläge des Bundesrates zugestimmt. In einer Reihe von wesentlichen Fragen hat sie sich dagegen eine Äußerung im weiteren Gesetzgebungsverfahren vorbehalten. Zu den Regelungskomplexen, in denen kein Konsens zwischen Bundesrat und Bundesregierung erzielt wurde, gehören namentlich

- die vom Bundesrat geforderte Schaffung angemessener Schutzvorschriften für die Datenverarbeitung in Akten auch im nicht-öffentlichen Bereich und eine Regelung der Datenerhebung im Bundesdatenschutzgesetz (Nr. 1 der Stellungnahme des Bundesrates),
- die Aufhebung der Privilegierung sog. interner Dateien (Nr. 3),
- der Auftrag des Bundesrates zu prüfen, ob das „Nutzen" personenbezogener Daten als Phase der Datenverarbeitung in die Legaldefinition der Datenverarbeitung einbezogen werden kann (Nr. 8),
- die Bindung der Einrichtung eines Direkt-Abrufverfahrens im öffentlichen Bereich an eine spezielle Rechtsvorschrift (Nr. 15),
- die Forderung des Bundesrates nach nur eingeschränkter Freistellung der Sicherheitsbehörden von der Auskunftspflicht (Nr. 27),
- die Erweiterung der Kontrolle durch den Bundesbeauftragten für den Datenschutz durch Einbeziehung der Datenerhebung (Nr. 32),
- die Stärkung und Erstreckung der Kontrollkompetenz der Aufsichtsbehörden auch auf die Verarbeitung personenbezogener Daten außerhalb von Dateien (Nr. 40ff.).

Die beabsichtigte Novellierung des Bundesdatenschutzgesetzes war auch Gegenstand von Anhörungen der zuständigen Arbeitskreise der Fraktionen der CDU/CSU und der SPD sowie des Innenausschusses des Deutschen Bundestages, bei denen ich Gelegenheit hatte, meine Stellungnahmen und Äußerungen zu den Gesetzentwürfen zu erläutern. Ich habe dabei auch deutlich gemacht, daß angesichts des seit der Entscheidung des Bundesverfassungsgerichts (Volkszählungsurteil) verstrichenen Zeitraums der Verabschiedung einer Novelle inzwischen höchste Dringlichkeit zukommt. Ich möchte darauf auch an dieser Stelle nachdrücklich hinweisen. Die in der noch nicht erfolgten Anpassung des BDSG an die veränderte verfassungsrechtliche Situation begründete Unsicherheit für die rechtliche Beurteilung der Datenverarbeitung sowohl bei den öffentlichen wie auch bei den privaten Stellen muß jetzt endlich durch die Schaffung eines der Rechtsprechung des Bundesverfassungsgerichts folgenden neuen Rechts beseitigt werden. Trotz der ebenfalls drängenden Probleme auf anderen Feldern der Politik appelliere ich an den Gesetzgeber, das

Gesetzgebungsverfahren noch in dieser Legislaturperiode abzuschließen. Anderenfalls droht dem Datenschutz insgesamt nicht nur bei unseren Bürgern, sondern auch bei den datenverarbeitenden Stellen ein erheblicher Verlust an Glaubwürdigkeit.

26 Nicht-öffentlicher Bereich

26.1 Zusammenarbeit mit den Aufsichtsbehörden der Länder

Über die wesentlichen datenschutzrechtlichen Fragenkomplexe aus dem Bereich der Privatwirtschaft habe ich in den vergangenen Jahren ausführlich berichtet (s. 10. TB S. 88ff., 11. TB S. 76ff.). An dem ständigen Meinungsaustausch zwischen den Datenschutz-Aufsichtsbehörden der Länder im „Düsseldorfer Kreis" habe ich mich auch im Berichtsjahr beteiligt.

Darüber hinaus bin ich vermehrt auch von Verbänden der Privatwirtschaft unmittelbar angesprochen und um meine Stellungnahme zu datenschutzrechtlichen Fragen gebeten worden. Dabei standen die beabsichtigte Novellierung des Bundesdatenschutzgesetzes und ihre Auswirkungen für die Datenverarbeitung der Privatwirtschaft stets im Vordergrund. Bei diesen Gesprächen und Diskussionen wurde erneut deutlich, daß Teile der Privatwirtschaft dem Gesetzentwurf der Bundesregierung skeptisch oder ablehnend gegenüberstehen. Dies gilt insbesondere für solche Wirtschaftszweige, für die personenbezogene Daten gleichsam der „Rohstoff" ihrer unternehmerischen Tätigkeit sind. Gegen den Gesetzentwurf wird vor allem eingewandt, daß eine verfassungsrechtliche Notwendigkeit, auch die für die Unternehmen geltenden Datenschutzbestimmungen fortzuentwickeln nicht bestehe, weil die Privatwirtschaft von der nach dem Volkszählungsurteil veränderten verfassungsrechtlichen Lage nicht betroffen sei; viele der vorgesehenen Bestimmungen schränkten die Möglichkeiten der Datenverarbeitung durch die Unternehmen stärker ein als dies verfassungsrechtlich zulässig sei oder führten, wie der vorgesehene Schadensersatzanspruch, zu Wettbewerbsnachteilen gegenüber den europäischen Mitbewerbern.

Wo immer sich mir im Rahmen des Dialogs mit Vertretern der Wirtschaft Gelegenheit bot, war ich bemüht, Verständnis und Offenheit für die notwendige Weiterentwicklung des Datenschutzes auch im Bereich der Privatwirtschaft zu wecken und zu entwikkeln, wobei ich stets für differenzierte, den berechtigten Belangen der Unternehmen, aber auch denen der Bürger, Rechnung tragende Regelungen eingetreten bin. Namentlich dort, wo der Bürger auf den Umgang mit den ihn betreffenden Informationen keinen mitgestaltenen Einfluß nehmen kann (s. 11. TB S. 87f.) ist eine Weiterentwicklung auch verfassungsrechtlich geboten. Ich habe darüber hinaus versucht, erneut deutlich zu machen, daß der Regierungsentwurf keineswegs schon alle Erwartungen des Datenschutzes befriedigt und in manchen Bereichen, so beim Adressenhandel und der Direktwerbung, hinter den Anforderungen der Datenschutzkonvention des Europarates und den dazu ergangenen Empfehlungen (s. 27.2) zurückbleibt. In meinen Gesprächen habe ich indessen auch die Überzeugung gewonnen, daß die betroffenen Unternehmen beim Inkrafttreten der Novelle in der Lage und bereit sind, für eine rasche Umsetzung des neuen Rechts zu sorgen. Sehr nachteilig würde es sich jedoch auswirken, wenn die jetzt schon seit Jahren andauernde Unsicherheit über die weitere Rechtsentwicklung nicht endlich durch die Verabschiedung eines neuen Gesetzes beendet würde.

26.2 Verbraucherkreditgesetz

Der Bundesminister der Justiz hat leider meine Anregung (s. 11. TB S.78) nicht aufgegriffen, in den Entwurf des Verbraucherkreditgesetzes auch Bestimmungen aufzunehmen, die die Verarbeitung von personenbezogenen Daten der Kreditnehmer bei der Eingehung und Abwicklung von Kreditverträgen sowie zur Kreditinformation und Bonitätskontrolle regeln. Da auch der Bundesrat in seiner Stellungnahme zu dem Gesetzentwurf auf die Aspekte des Umgangs mit personenbezogenen Informationen nicht eingegangen ist, sind die demnächst beginnenden Ausschußberatungen des Bundestages die letzte Gelegenheit zur datenschutzrechtlichen Ergänzung des Gesetzgebungsvorhabens.

In der Sache geht es in erster Linie darum, präzise zu bestimmen, welche personenbezogenen Angaben bei der Eingehung eines Kredits vom Kreditgeber erhoben und für welche Zwecke diese Daten gespeichert, weiter verarbeitet, übermittelt oder sonst genutzt werden dürfen. Angesichts der inzwischen vorhandenen mannigfaltigen Formen des Verbraucherkredits (z. B. Ratenkredit, Rahmenkredit, Ratenkauf, Zielkauf, Leasing, Kreditkarten) und seiner sowohl volkswirtschaftlich wie auch individuell großen Bedeutung ist dabei die Datenverarbeitung für Zwecke der Kreditinformation von besonderem Interesse. Der rechtliche Rahmen, innerhalb dessen sich die Bonitätsprüfung zur Kreditentscheidung und -überwachung (kontinuierliche Bonitätskontrolle bei bestehenden Kreditverpflichtungen) bewegen darf, muß gesetzlich bestimmt werden. Dazu gehören auch Regelungen über den Umfang der Nutzung von Daten, die aus gerichtlichen und außergerichtlichen Streitigkeiten infolge nicht vertragsgemäßer Abwicklung von Verbraucherkrediten stammen.

Ich habe die Aufsichtsbehörden der Länder in meine Gespräche mit dem Bundesminister der Justiz einbezogen, um die von diesen gewonnenen Erfahrungen aus der Praxis zu nutzen.

27 Ausland und Internationales

Eine bemerkenswerte Entwicklung hat das Jahr 1989 auf dem Gebiet des internationalen Datenschutzes gebracht. Eine Reihe von Ereignissen und Maßnahmen, auf die im folgenden näher eingegangen werden soll, belegt, daß in weitem Umfang erkannt worden ist, welche entscheidende Bedeutung die internationalen Aspekte in den kommenden Jahren gerade

auch für den Datenschutz haben werden. Erstmals hat sich die internationale Datenschutzkonferenz ganz auf ein Thema — den grenzüberschreitenden Datenverkehr — konzentriert und in einer Entschließung auf den großen Handlungsbedarf auf diesem Gebiet hingewiesen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist — ebenso wie die Konferenz der obersten Aufsichtsbehörden für den nicht-öffentlichen Bereich (Düsseldorfer Kreis) — dabei, einen besonderen Arbeitskreis für internationale Fragen zu bilden. Seit dem Datenschutzübereinkommen des Europarats von 1981 wurde erstmals ein weiterer völkerrechtlicher Vertrag mit umfangreichen Regelungen zum Datenschutz erarbeitet: das Schengener Zusatzübereinkommen. Nach der Verabschiedung von Datenschutzgesetzen in Australien und Japan und einer entsprechenden Ankündigung aus Ungarn steht der Datenschutz heute an der Schwelle seiner weltweiten Ausbreitung.

27.1 Zusammenarbeit der Datenschutz-Kontrollinstanzen — Elfte Internationale Konferenz der Datenschutzbeauftragten in Berlin —

Die Internationale Datenschutzkonferenz hat im Jahre 1989 unter deutscher Präsidentschaft Ende August in Berlin im Reichstagsgebäude stattgefunden. Der Berliner Datenschutzbeauftragte hat sich an der Organisation der Konferenz maßgeblich beteiligt. Teilnehmer waren Vertreter von über dreißig Datenschutz-Kontrollinstanzen (einschließlich solcher von Bundesländern und vergleichbaren Teilstaaten), Regierungsvertreter aus acht Ländern und Repräsentanten von vier internationalen Organisationen sowie Wissenschaftler, Publizisten Verbandsvertreter und weitere Fachleute — insgesamt etwa 130 Personen.

Die Konferenz stand unter dem Motto „Datenflüsse ohne Grenzen — neue Aufgaben für den Datenschutz". Erörtert wurden die gesetzlichen Regelungen der verschiedenen Länder zur Problematik des grenzüberschreitenden Datenverkehrs, die internationalen Instrumente des Datenschutzes (Datenschutzkonvention des Europarats, Datenschutz-Leitlinien der OECD und Datenschutzgrundsätze der Vereinten Nationen) und sektorale Schwerpunkte (Statistik, polizeiliche Fahndung). Die Verhandlungen ergaben völlige Übereinstimmung, daß es angesichts des inzwischen erreichten Umfangs des grenzüberschreitenden Datenverkehrs dringend geboten ist, die Bemühungen um den internationalen Datenschutz zu verstärken. Da Länder mit Datenschutzgesetzen weltweit noch klar in der Minderheit sind und auch Europa von einem flächendeckenden Datenschutz noch weit entfernt ist, bedeutet die Übermittlung von Daten ins Ausland für den Betroffenen in der großen Mehrzahl der Fälle heute immer noch, daß er im Empfängerland weder die Richtigkeit und Zulässigkeit der Verarbeitung seiner Daten prüfen noch die Zwecke ihrer Verwendung kontrollieren und auch keinen unabhängigen Datenschutzbeauftragten anrufen kann. Die Datenschutzbeauftragten haben deshalb in einer Entschließung die Regierungen aufgefordert, einzeln und im Rahmen internationaler Organisationen darauf hinzuarbeiten, daß in allen Ländern ein gleichwertiger gesetzlicher Datenschutz auf der Grundlage der Datenschutzkonvention des Europarats und der OECD-Leitlinien geschaffen wird. International operierende Datenverarbeitungssysteme sollen so aufgebaut werden, daß der einzelne ohne unzumutbare Schwierigkeiten seine Datenschutzrechte auch im Ausland wahrnehmen kann. Die Datenschutzbeauftragten der Länder der Europäischen Gemeinschaft haben darüber hinaus in einer gesonderten Erklärung die Gemeinschaft und die Mitgliedstaaten aufgefordert, in ihre Planungen für den Europäischen Binnenmarkt den Datenschutz mit aufzunehmen. Insbesondere sollen die Datenschutzkonvention des Europarats für alle Mitgliedstaaten wie auch für die Institutionen der Gemeinschaft selbst verbindlich gemacht und eine unabhängige Datenschutz-Kontrollinstanz auf europäischer Ebene eingerichtet werden. Daneben hat die internationale Datenschutzkonferenz Grundsätze für offene Telekommunikationsnetze beschlossen. Die Beschlüsse der Konferenz sind als Anlage 12 abgedruckt.

Die praktische Zusammenarbeit zwischen den Datenschutz-Kontrollinstanzen hat sich weiter vertieft. In zunehmendem Umfang wird sowohl bei Beratungsaufgaben als auch bei der rechtlichen Beurteilung von Sachverhalten im Rahmen der Kontrolle von der Möglichkeit Gebrauch gemacht, die Erfahrungen der Partnerorganisationen abzufragen. Außerordentlich nützlich war auch die Zusammenarbeit zwischen den Datenschutz-Institutionen der Schengen-Länder. Ihre im März 1989 formulierte gemeinsame Position zu den datenschutzrechtlichen Grundsatzfragen, die das geplante Schengener Informationssystem aufwirft, wurde von den Regierungen weitestgehend akzeptiert und hat in den Regelungen des Vertragsentwurfs konkreten Niederschlag gefunden. Die Tatsache, daß der Datenschutz mit einem Munde sprach, erleichterte die Einigung bei den Verhandlungen der Regierungen, verstärkte aber sichtbar zugleich das Gewicht des Datenschutzes (zur Sache vergleiche unten 27.6).

27.2 Europarat

Nachdem im abgelaufenen Jahr Dänemark die Datenschutzkonvention des Europarats (Konvention 108) ratifiziert hat, sind nunmehr die folgenden neun Länder Vertragsparteien: Schweden, Norwegen, Frankreich, Bundesrepublik Deutschland, Spanien, Österreich, Luxemburg, Großbritannien und Dänemark. Weitere Beitritte werden in naher Zukunft erwartet.

Der Europarat setzt seine Politik fort, die Datenschutzkonvention durch bereichsspezifische Empfehlungen zu ergänzen. Bis zum Jahresende 1989 waren folgende Empfehlungen verabschiedet:

— Empfehlung über medizinische Datenbanken (R(81)1)

— Empfehlung zum Schutz personenbezogener Daten für Zwecke der wissenschaftlichen Forschung und Statistik (R(83)10)

- Empfehlung zum Schutz personenbezogener Daten bei der Verwendung für Zwecke der Direktwerbung (R(85)20)
- Empfehlung zum Schutz personenbezogener Daten in der sozialen Sicherung (R(86)1)
- Empfehlung über den Datenschutz bei der Verarbeitung personenbezogener Angaben im Polizeisektor (R(87)15)
- Empfehlung über Datenschutz und Informationsfreiheit (R(86)1037)
- Empfehlung über den Schutz personenbezogener Daten für Beschäftigungszwecke (R(89)2).

Eine Empfehlung zum Schutz personenbezogener Daten beim Zahlungsverkehr und damit verbundenen Vorgängen steht zur Verabschiedung an. Weitere Arbeitsschwerpunkte des Expertenausschusses für Datenschutz des Europarats liegen auf den Gebieten technologischer Wandel und Telekommunikation, Personen-Identifizierungsnummern, öffentliche Datenbestände, medizinische Daten, personenbezogene Datenverarbeitung in den Bereichen Medien, Volkszählung und Versicherungen.

27.3 Datenschutz in der Europäischen Gemeinschaft

Eines der wesentlichen Ergebnisse der internationalen Datenschutzkonferenz in Berlin ist die gemeinsame Auffassung aller Datenschutz-Kontrollinstanzen der Länder der Europäischen Gemeinschaft, daß der Datenschutz nicht länger aus dem Wirken der Gemeinschaft ausgeklammert bleiben darf. Schon zu dem Ziel, Wettbewerbsverzerrungen und das Entstehen von Datenverarbeitungsoasen zu verhindern, muß die Gemeinschaft an einem ausgeglichenen Datenschutzniveau interessiert sein. Dies wird offensichtlich auch von der Kommission so gesehen. Sie hat in den vergangenen Jahren die Mitgliedsländer wiederholt aufgefordert, die Europaratskonvention zu ratifizieren. Der Erfolg war gering. Nach wie vor verfügen folgende EG-Länder über kein oder kein umfassendes Datenschutzgesetz und können demgemäß der Konvention nicht beitreten: Belgien, Niederlande, Portugal, Italien und Griechenland. Hinzu kommt, daß Spanien ratifiziert hat, ohne ein Datenschutzgesetz zu haben. Bei manchen dieser Länder besteht wenig Grund zu der Hoffnung, daß sie in absehbarer Zeit ein Datenschutzgesetz erlassen, wenn sie nicht entsprechende Anstöße von außen erhalten. Eine Gemeinschaftsinitiative für den Datenschutz ist — unabhängig von der wirtschaftspolitischen Sicht — heute dringend notwendig, um das Europa der Bürger voranzubringen.

Die Beschlüsse der Internationalen Datenschutzkonferenz von Berlin sind den Organen der Gemeinschaft unterbreitet worden. Die Überlegungen innerhalb der Kommission, ob eine Datenschutz-Initiative ergriffen werden soll und wie diese auszusehen hätte, befinden sich aber nach meiner Kenntnis noch ganz in den Anfängen. Die negativen Erfahrungen der vergangenen Jahre haben gezeigt, daß die bisherigen Bemühungen noch erheblich verstärkt werden müssen.

Die Gemeinschaft muß auch selbst institutionell Vorsorge für den Datenschutz treffen. Nachdem der Europarat und die OECD interne Datenschutzregelungen erlassen und Datenschutz-Kontrollinstanzen eingerichtet haben, kann die Gemeinschaft, die über einen ungleich größeren Verwaltungsbereich mit einem entsprechend größeren Umfang personenbezogener Datenverarbeitung verfügt, nicht länger untätig bleiben. Nicht nur die Datenschutzbeauftragten der Mitgliedsländer der Gemeinschaft, sondern auch die Organe der Gemeinschaft, ihre Verwaltungseinrichtungen und ihre Mitarbeiter brauchen dringend einen europäischen Datenschutzbeauftragten. Die vielfältigen und umfangreichen Aktivitäten der Gemeinschaft, etwa auf den Gebieten der Informationstechnik, der Forschung und der Medizin — um nur einige Beispiele zu nennen —, verlangen, daß systematisch geprüft wird, welche Implikationen für den Datenschutz sie haben, und daß Grundsätze und Maßnahmen des Datenschutzes in zielgerichteter und konsistenter Weise entwickelt werden. So hätte es beispielsweise nahegelegen, in die kürzlich verabschiedete Sozialcharta den Arbeitnehmerdatenschutz mit aufzunehmen. Auch die von der Gemeinschaft angestrebte Möglichkeit der Weitergabe statistischer Einzelangaben von den nationalen Statistikämtern an das Statistische Amt der EG setzt voraus, daß dort eine Datenschutzkontrolle besteht (vgl. Anlage 9). Ohne eine besondere Institution, die den notwendigen Sachverstand bündelt und den Datenschutz durch Beratung und Kontrolle praktisch voranbringt, wird die Gemeinschaft zwangsläufig noch weiter hinter das europäische Datenschutzniveau zurückfallen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung vom 26./27. Oktober 1989 (s. Anlage 8) auf den dringenden Handlungsbedarf hingewiesen. Ich appelliere erneut an die Bundesregierung wie auch an die Verantwortlichen in den Organen der Gemeinschaft, geeignete Schritte zu unternehmen, um den Datenschutz in der Europäischen Gemeinschaft Wirklichkeit werden zu lassen. Insbesondere sollte die Bundesregierung ihr Engagement verstärken. Bloßes Interesse daran, „daß auch die Rechtsakte der EG Bestimmungen enthalten, die den Erfordernissen des Datenschutzes in geeigneter Weise Rechnung tragen" (vgl. die Antwort der Bundesregierung auf die Große Anfrage zu den Innenpolitischen Aspekten der Fortentwicklung der EG, BT-Drucksache 11/5615 S. 5f.) reicht nicht aus, einen entscheidenden datenschutzrechtlichen Fortschritt im EG-Bereich zu erzielen.

27.4 Vereinte Nationen

Auch die Vereinten Nationen haben sich mit dem Datenschutz beschäftigt. Im vergangenen Jahr hat die Menschenrechtskommission „Richtlinien über automatisierte Personendateien" beschlossen. Die Generalversammlung hat in ihrer 44. Sitzung am 15. November 1989 die Menschenrechtskommission aufgefordert, diese Richtlinien unter Berücksichtigung der Stellungnahmen von Mitgliedsstaaten und internatio-

nalen Organisationen erneut zu beraten und — soweit erforderlich — mit entsprechenden Änderungen über den Wirtschafts- und Sozialausschuß der Generalversammlung zur 45. Sitzung zur endgültigen Beschlußfassung erneut zuzuleiten.

Diese Richtlinien verstehen sich als Vorgabe für die Gesetzgebung der einzelnen Länder wie auch für Regelungen internationaler Organisationen. Es ist bemerkenswert, daß die Richtlinien der Vereinten Nationen nicht den Charakter eines Minimalkonsenses haben, sondern in mehreren Punkten durchaus richtungweisend wirken. So wird beispielsweise ein Verbot der Speicherung von Daten empfohlen, die mit einer gewissen Wahrscheinlichkeit für ungesetzliche oder willkürliche Maßnahmen verwendet werden könnten (Verbot diskriminierender Daten). Ein besonderer Schwerpunkt liegt bei der Zweckbestimmung und Zweckbindung von Daten; der Umfang der Speicherung, die Weitergabe und die Speicherdauer müssen sich an dem Zweck der Datenspeicherung orientieren, der legitim sein muß und schon vor der Speicherung spezifiert festgelegt und öffentlich bekanntgegeben werden muß. Die Notwendigkeit einer Kontrollinstanz mit garantierter Unabhängigkeit und technischer Kompetenz gehört zu den unverzichtbaren Elementen einer Datenschutzregelung. Schließlich wird auch gefordert, die manuelle Verarbeitung personenbezogener Daten — mit entsprechenden Anpassungen — in die gesetzliche Regelung einzubeziehen. Der Text der Richtlinien ist als Anlage 14 abgedruckt.

27.5 Entwicklung des Datenschutzes im Ausland

Seit Ende 1988 verfügt auch Japan über ein nationales Datenschutzgesetz. Die Vertreter Ungarns haben auf der Internationalen Datenschutzkonferenz in Berlin angekündigt, ihr Land werde in Kürze ein Datenschutzgesetz verabschieden und der Datenschutzkonvention des Europarates beitreten. Nachdem 1988 schon Australien ein nationales Datenschutzgesetz geschaffen hatte, verstärkt sich nun die geographische Basis des Datenschutzes deutlich. Zieht man noch die jüngsten Aktivitäten der Vereinten Nationen in Betracht, so läßt sich feststellen, daß der Datenschutz im Begriff ist, aus seinen westeuropäischen Stammlanden herauszutreten und weltweit anerkannt zu werden.

In vielen Ländern liegt der Schwerpunkt der Aktivitäten inzwischen im bereichsspezifischen Datenschutz. Einige Länder sind auch bemüht, parallel zu einem allgemeinen Datenschutzgesetz bereichsspezifische Regelungen zu entwickeln. Schwerpunkte liegen dabei in den Bereichen Verbraucherkredit (Belgien, Österreich und Australien), Personenkennzeichen und Bevölkerungsregister (Niederlande, Schweden, Kanada) und Polizei (Niederlande, Schweden). Dabei zeigt sich, daß die bereichsspezifischen Empfehlungen des Europarats zunehmende Bedeutung als Richtschnur für nationale Aktivitäten gewinnen. Die Fortentwicklung bestehender Datenschutzgesetze folgt weiterhin den schon bekannten Linien der Spezialisierung, der Verstärkung der Datenschutzinstanzen durch bessere Befugnis und Entlastung von Routine sowie der Anpassung an die technische Entwicklung.

27.6 Schengener Übereinkommen

Im Schengener Übereinkommen vom 14. Juni 1985 haben die Regierungen der Staaten der Benelux-Wirtschaftsunion, der französischen Republik und der Bundesrepublik Deutschland vereinbart, die Kontrollen an den gemeinsamen Grenzen schrittweise abzubauen. Auf der Grundlage dieser Vereinbarung wurde im Berichtsjahr der Entwurf eines Staatsvertrages (des sog. Schengener Zusatzübereinkommens) ausgehandelt, in dem eine engere Zusammenarbeit zwischen den Behörden der beteiligten Staaten vereinbart wird. Damit soll eine Art Ausgleich für die wegfallenden Grenzkontrollen geschaffen werden. Dazu gehören eine verstärkte und abgestimmte Kontrolle an den Außengrenzen des Schengener Gebiets sowie eine intensivere Zusammenarbeit der Vertragsstaaten auf verschiedenen Gebieten der Justiz und der Verwaltung. Schwerpunkte liegen bei der Strafverfolgung, bei der polizeilichen Gefahrenabwehr, beim Ausländerrecht, beim Asylrecht, beim Betäubungsmittelrecht und beim Waffenrecht. Als Kernstück betrachten die Vertragsstaaten das geplante Schengener Informationssystem (S.I.S.), einen gemeinsamen polizeilichen Fahndungsdatenbestand, der über je eine zentrale Behörde der Vertragsstaaten beschickt und in identischer Form den zuständigen Behörden für Kontrollen an den Außengrenzen wie auch im Binnenland zum direkten Abruf zur Verfügung stehen soll.

Die datenschutzrechtlichen Voraussetzungen in den beteiligten Ländern sind sehr unterschiedlich. Frankreich und die Bundesrepublik Deutschland verfügen seit über einem Jahrzehnt über ein voll ausgebautes Datenschutzsystem. Beide Länder haben die Datenschutzkonvention des Europarats ratifiziert. Dies gilt auch für Luxemburg, dessen Datenschutzgesetz von 1979 allerdings kein unabhängiges Kontrollorgan vorsieht, sondern lediglich einen beratenden Ausschuß. Die Niederlande haben seit dem abgelaufenen Jahr zwar ein Datenschutzgesetz, das aber nicht für die Polizei gilt. Ein Spezialgesetz für diesen Bereich soll 1990 folgen. Belgien hat Datenschutzbestimmungen für einige Spezialbereiche, jedoch kein allgemein gültiges nationales Datenschutzgesetz.

Unter diesen Bedingungen konnte ich der in den Regierungsverhandlungen ursprünglich verfolgten Konzeption, die Regelung des Datenschutzes im wesentlichen den Vertragsstaaten zu überlassen, nicht zustimmen. Es genügt auch nicht, den Datenschutz nur insoweit im Abkommen festzulegen, als aus technisch-organisatorischen Gesichtspunkten eine einheitliche Verfahrensweise erforderlich ist. Ein international operierendes Informationssystem mit so großer Bedeutung für die Rechte des einzelnen darf vielmehr nur dann eingerichtet werden, wenn ein effektiver Datenschutz für das gesamte System sichergestellt ist. Dies ist auch die Position der Datenschutzinstanzen Frankreichs und Luxemburgs. Zusammen mit diesen habe ich in einer gemeinsamen Erklärung vom 16. März 1989 in diesem Sinne Mindestbedingungen

aufgestellt, die vor Inbetriebnahme des Systems erfüllt sein müssen (abgedruckt als Anlage 13). Dazu gehören vor allem eine rechtsverbindliche Bestimmung des Dateiinhalts und der Datenverwendung, eine Garantie, daß die Betroffenen ihre Datenschutzrechte in allen Ländern ausüben können, die Gewährleistung einer unabhängigen Datenschutzkontrolle in den einzelnen Vertragsstaaten sowie die Installierung eines gemeinsamen Kontrollorgans für übergreifende Kontrollaufgaben.

Diese Forderungen wurden von der Bundesregierung als Verhandlungsziel übernommen und sind in der im Dezember 1989 erreichten Formulierung des Vertragsentwurfs, soweit es um das Schengener Informationssystem geht, weitestgehend realisiert. So verpflichten sich die Vertragsparteien, spätestens bis zum Inkrafttreten des Übereinkommens in ihrem nationalen Recht die erforderlichen Maßnahmen zu treffen, um die Grundsätze der Datenschutzkonvention des Europarats sowie der Empfehlung des Ministerausschusses des Europarats zum Datenschutz im Polizeibereich vom 17. September 1987 zu verwirklichen (Artikel 118 des Entwurfs). Jede Vertragspartei muß auch eine unabhängige Kontrollinstanz besitzen, deren Aufgabe darin besteht, den nationalen Schengener Datenbestand zu überwachen (Artikel 115). Zur Kontrolle des zentralen Datenbestandes, der voraussichtlich in Straßburg geführt werden soll, und zur Behandlung übergreifender datenschutzrechtlicher Fragen soll eine gemeinsame Kontrollinstanz eingerichtet werden, die sich aus je zwei Vertretern der nationalen Kontrollinstanzen zusammensetzt (Artikel 116). Nach längeren Verhandlungen wurde auch eine Regelung durchgesetzt, die dem Betroffenen unabhängig von seiner Nationalität und seinem Wohnsitz das Recht gibt, in jedem Vertragsstaat Auskunft über die zu seiner Person gespeicherten Daten zu erhalten. Insgesamt betrachte ich die Regelungen zum Schengener Informationssystem — von wenigen Schwachstellen abgesehen — als eine tragfähige Lösung, der auch Modellcharakter für andere internationale Informationssysteme zukommt.

Demgegenüber sind die datenschutzrechtlichen Regelungen für die internationale Zusammenarbeit, die außerhalb des Schengener Informationssystems in konventionellen Formen ablaufen soll, noch nicht voll befriedigend. Zwar gibt es für drei Bereiche ausdrückliche datenschutzrechtliche Regelungen, so für den Austausch von Daten von Asylbewerbern (Artikel 38), für die Übermittlung personenbezogener Daten zum Zwecke der polizeilichen Gefahrenabwehr (Artikel 46) und für die Unterrichtung über Waffenerwerber (Artikel 92). Diese Regelungen sind jedoch untereinander nicht abgestimmt, was zu Schwierigkeiten bei der Anwendung führen kann. Die Regelungen zum Asyl- und zum Waffenrecht verweisen darüber hinaus — und zwar in unterschiedlicher Weise — auf das jeweilige nationale Recht, ohne inhaltliche Grundsätze vorzugeben. Vor allem aber sieht der Entwurf für einige Bereiche eine intensive Zusammenarbeit vor, die auch einen grenzüberschreitenden Austausch personenbezogener Daten umfaßt, ohne daß insoweit datenschutzrechtliche Vorkehrungen getroffen werden. Dies gilt insbesondere für das Ausländerrecht, die Zusammenarbeit der nationalen Sicherheitsdienste sowie die Kontrolle des Transports von Gefahrgütern und der Ausfuhr von strategischen Industriewaren und Technologien. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hatte in einer Entschließung vom 26./27. Oktober 1989 besonders darauf hingewiesen, daß Regelungen über den Datenschutz auch auf die im Zusatzübereinkommen vorgesehene konventionelle Datenverarbeitung ausgedehnt werden müssen (abgedruckt als Anlage 6). Ich stehe mit den Datenschutzinstanzen der Schengener Vertragsstaaten und mit den zuständigen deutschen Stellen in Verbindung, um noch eine entsprechende Verbesserung des Vertragsentwurfs zu erreichen.

28 Bilanz

Auch diese Bilanz zeigt, daß für viele der im vergangenen Berichtsjahr aufgeworfenen Fragen befriedigende Antworten gefunden werden konnten. In anderen Bereichen konnten dagegen Probleme noch nicht gelöst werden.

1. Auf ungelöste Fragen bei der ärztlichen Untersuchung von Asylbewerbern habe ich hingewiesen (11. TB S. 16). Die Diskussion über eine Lösung dauert an; siehe dazu Nr. 3.4.1 in diesem Bericht.
2. Zu dem geplanten Gesetz über das Ausländerzentralregister habe ich eine Vielzahl von datenschutzrechtlichen Forderungen gestellt (11. TB S. 16 f.). Der intensive Dialog mit dem Bundesminister des Innern hat zu erheblichen Verbesserungen im inzwischen vorliegenden Regierungsentwurf geführt; siehe dazu Nr. 3.2.2 in diesem Bericht.
3. Für eine datenschutzgerechte Organisation der Datenverarbeitung bei der Bundesanstalt Technisches Hilfswerk (THW) habe ich Anregungen gegeben (11. TB S. 18 f.). Der Bundesminister des Innern hat meine Anregungen aufgegriffen; siehe dazu Nr. 3.7 in diesem Bericht.
4. Eine gesetzliche Festlegung der Aufbewahrungsdauer für Unterlagen aus dem Anerkennungsverfahren für Kriegsdienstverweigerer habe ich gefordert (11. TB S. 19). Mit dem Zweiten Gesetz zur Änderung des Kriegsdienstverweigerungs-Neuordnungsgesetzes ist eine datenschutzgerechte Regelung getroffen worden; siehe dazu Nr. 3.6.1 in diesem Bericht.
5. Über die Bereitschaft des Bundesministers der Justiz, Verbesserungen der Datenschutzbestimmungen des Bundeszentralregistergesetzes vorzunehmen, habe ich berichtet (11. TB S. 19f.). Nach gemeinsamen Besprechungen mit dem Bundesminister der Justiz und den Justizverwaltungen der Länder gehe ich davon aus, daß etwa Mitte 1990 ein deren Ergebnisse berücksichtigender neuer Arbeitsentwurf vorgelegt werden wird.
6. Im Rahmen der Diskussion über die Novellierung der Strafprozeßordnung habe ich insbesondere

auf die Problematik überregionaler Datensammlungen über Strafverfahren hingewiesen (11. TB S. 20). An den weiteren Erörterungen habe ich mich beteiligt; eine auch aus Datenschutzgründen gebotene hinreichende Koordinierung der staatsanwaltschaftlichen mit der entsprechenden polizeilichen Datenverarbeitung ist jedoch noch nicht erreicht; siehe dazu Nr. 4.1 in diesem Bericht.

7. Auf Probleme, die sich aus der Zusammenfassung der Entscheidungen über unterschiedliche Sachverhalte in Ehescheidungsverbundurteilen ergeben, habe ich aufmerksam gemacht (11. TB S. 21 f.). Meine Bemühungen haben Verständnis gefunden, die Diskussion hat aber noch zu keinen konkreten Lösungen geführt; siehe dazu Nr. 4.2.4 in diesem Bericht.

8. Der Informationszentrale für Auslandsbeziehungen (IZA), einer Organisationseinheit des Bundesamtes für Finanzen, habe ich im Rahmen einer datenschutzrechtlichen Kontrolle zur Erfüllung von Anforderungen, die das Bundesdatenschutzgesetz in Verfahrensfragen stellt, eine Reihe von Verbesserungen empfohlen (11. TB S. 22). Die IZA ist meinen Empfehlungen im wesentlichen gefolgt.

9. Verzögerungen beim Erlaß einer Rechtsverordnung für Mitteilungen von Behörden und öffentlich-rechtlichen Körperschaften an Finanzämter über Zahlungen z. B. an nebenberuflich tätige Personen wie Vortragende, Übersetzer oder Gutachter habe ich bedauert (11. TB S. 23). Der Bundesminister der Finanzen beabsichtigt, die Verordnung im Sommer 1990 zu erlassen.

10. Über meine Mitwirkung am Entwurf der Steuerdaten-Abruf-Verordnung habe ich berichtet (11. TB S. 23f.). Auch in der strittigen Frage der Datenabrufberechtigung der Oberfinanzbehörden zeichnet sich eine datenschutzgerechte praktikable Lösung ab; siehe dazu Nr. 5.2 in diesem Bericht.

11. Zur Personaldatenverarbeitung beim Deutschen Patentamt habe ich verschiedene Empfehlungen gegeben (11. TB S. 24 f.). Das Deutsche Patentamt hat einige meiner Empfehlungen umgesetzt.

12. Über die Ergebnisse meiner Mitwirkung in der interministeriellen Arbeitsgruppe zur Neuordnung des Personalaktenwesens habe ich berichtet (11. TB S. 25f.). Gegen Ende des Berichtsjahres hat der Bundesminister des Innern einen Referentenentwurf zur Novellierung des Bundesbeamtengesetzes und des Beamtenrechtsrahmengesetzes vorgelegt, der zwar einige datenschutzfreundliche Regelungen enthält, auf die besonderen Gefahren der automatisierten Verarbeitung von Personaldaten der Beamten aber nicht hinreichend eingeht und in weiteren wesentlichen Punkten, z. B. in der Frage der konkreten Zweckbindung, noch verbesserungsbedürftig ist.

13. Über meine Mitwirkung am Entwurf der Neufassung der Dienstanschlußvorschriften habe ich berichtet (11. TB S. 26 f.). Der Bundesminister für Finanzen hat den Entwurf inzwischen fertiggestellt, so daß diese Vorschriften voraussichtlich im Frühjahr 1990 in Kraft treten werden.

14. Zur Lösung datenschutzrechtlicher Probleme bei einem Verfahren zur automatisierten Fahrkartenausgabe habe ich Anregungen gegeben (11. TB S. 27 f.). Bei der weiteren Ausgestaltung des Verfahrens hat die Deutsche Bundesbahn diese aufgegriffen.

15. Zum Aufbau von Personalinformationssystemen bei der Deutschen Bundesbahn habe ich mehrere Anregungen gegeben (11. TB S. 28 f.), die die Deutsche Bundesbahn aufgegriffen hat.

16. Bei der Neustrukturierung des Post- und Fernmeldewesens habe ich vor allem gefordert, daß auch bei den privaten Anbietern postalischer Dienstleistungen der Datenschutz mindestens auf dem gegenwärtigen Niveau gewährleistet sein müsse (11. TB S. 30). Die mittlerweile in Kraft getretenen gesetzlichen Vorschriften haben die Voraussetzung dafür geschaffen; siehe dazu Nr. 7.1 in diesem Bericht.

17. Bei der Verarbeitung von Verbindungsdaten im Funktelefondienst — C-Netz — habe ich verschiedene Mängel festgestellt (11. TB S. 30 ff.). Für die Übermittlungen und die Zugriffe auf diese Daten sind jetzt restriktive Regelungen getroffen worden. Die von mir beanstandete Speicherung aller Verbindungsdaten für etwa drei Monate wird aber fortgesetzt; siehe dazu Nr. 7.3.1 in diesem Bericht.

18. Über die Speicherung der Telefonverbindungsdaten im Rahmen des ISDN-Pilotversuches der Deutschen Bundespost habe ich berichtet (11. TB S. 32 f.). Nach einer Kontrolle der Kommunikationsdatenverarbeitung habe ich die auch im Regelbetrieb etwa drei Monate dauernde Speicherung der Verbindungsdaten aller von ISDN-Anschlüssen geführten Telefongespräche beanstandet; siehe dazu Nr. 7.2.3 in diesem Bericht.

19. Über Mängel beim Einsatz von Arbeitsplatzcomputer (APC) in einem Fernmeldeamt habe ich berichtet (11. TB S. 35). Eine Kontrolle in einem weiteren Fernmeldeamt zeigte auch dort Organisationsdefizite beim APC-Einsatz. Der Bundesminister für Post und Telekommunikation bemüht sich jedoch ernsthaft, durch Regelungen und Maßnahmen Abhilfe zu schaffen; siehe dazu Nr. 24.2.2 in diesem Bericht.

20. Zur Vermeidung von fehlerhaften Auskünften durch das Kraftfahrt-Bundesamt über die Halter von Kraftfahrzeugen habe ich geeignete organisatorische und technische Maßnahmen gefordert (11. TB S. 38). Das Kraftfahrt-Bundesamt hat inzwischen Verbesserungen an dem Verfahren zur Aktualisierung der Daten vorgenommen, über deren Auswirkungen mir noch keine konkreten Erfahrungen vorliegen.

21. Auf beim Kraftfahrt-Bundesamt bestehende Mängel bei der aus Sicherheitsgründen vorgenommenen Auslagerung von Magnetbandkopien habe ich wiederholt hingewiesen (11. TB S. 94, Nr. 21).

Inzwischen sind für die Sicherheitsauslagerung eine zufriedenstellende Lösung realisiert und erfolgsversprechende Vorarbeiten für einen Wiederanlauf der Datenverarbeitung nach schweren Betriebsstörungen durchgeführt worden.

22. Auf datenschutzrechtliche Defizite bei der Bundesanstalt für Straßenwesen habe ich hingewiesen (11. TB S. 38f.). Über die zur Beseitigung der Mängel erforderlichen Konzepte zum Datenschutz und zur Datensicherung sowie über die gebotenen Änderungen in der Organisationsstruktur bin ich bisher nicht unterrichtet worden. Zu einer weiteren Kontrolle dort siehe Nr. 6.1 in diesem Bericht.

23. Auf datenschutzrechtliche Probleme bei der Verwendung von Adreßdateien zur Verknüpfung von Wirtschafts- und Umweltstatistiken habe ich hingewiesen (11. TB S. 40f.). Der jetzt gefundene Kompromiß ist inhaltlich tragbar. Eine gesetzliche Regelung steht noch aus; siehe dazu Nr. 9.1 in diesem Bericht.

24. Gegen einzelne Regelungen im Entwurf des Agrarstatistikgesetzes habe ich Bedenken geltend gemacht (11. TB S. 41f.). Im Gesetzgebungsverfahren konnte eine zufriedenstellende Lösung gefunden werden; siehe dazu Nr. 9.2 in diesem Bericht.

25. In dem Novellierungsentwurf zum Umweltstatistikgesetz habe ich die vorgesehene Erlaubnis kritisiert, Einzelangaben in Tabellen für Planungszwecke an die zuständigen obersten Bundes- und Landesbehörden zu übermitteln und bestimmte Einzelangaben zu veröffentlichen (11. TB S. 43). Ich habe erreicht, daß die kritisierte Regelung im Entwurf gestrichen wurde.

26. Gegen eine vom Bundesrat bei der Novellierung des Straßenverkehrsunfallstatistikgesetzes angestrebte Regelung, nach der Einzelangaben an bestimmte Länderbehörden weitergegeben werden könnten, habe ich Bedenken angemeldet (11. TB S. 43f.). Die Bundesregierung hat in ihrer Gegenäußerung zur Stellungnahme des Bundesrates die datenschutzrechtlich bedenklichen Änderungswünsche zurückgewiesen.

27. Über die im Rahmen des Gesundheits-Reformgesetzes erfolgte Neufassung der Vorschriften über die Krankenhausstatistik habe ich berichtet (11. TB S. 44f.). Die Bundesregierung hat dazu eine Rechtsverordnung beschlossen, die den datenschutzrechtlichen Anforderungen genügt.

28. Die Ausländerstatistik betreffende Regelungen im Entwurf eines Gesetzes über das Ausländerzentralregister habe ich kritisiert (11. TB S. 45). Die Beratungen mit dem BMI haben in einigen Punkten schon zu tragbaren Ergebnissen geführt; siehe dazu Nr. 9.3 in diesem Bericht.

29. Eine Lösung datenschutzrechtlicher Fragen der Todesursachenstatistik im Rahmen der Novellierung des Bevölkerungsstatistikgesetzes habe ich gefordert (11. TB S. 47). Gegen den vom BMI erarbeiteten Entwurf bestehen Bedenken.

30. Zu datenschutzrechtlichen Problemen bei der Einführung eines „Informationstechnischen Systems zur Unterstützung bei Kostenrechnungen im Dienstrechtsbereich (ISKD)" habe ich Anregungen gegeben (11. TB S. 47). Der BMI hat diese Anregungen aufgegriffen und insbesondere Aggresationsverfahren so angelegt, daß die nachträgliche Wiederherstellung eines Personenbezuges nicht möglich ist.

31. Für einen Verzicht der Bundesanstalt für Arbeit auf einen detaillierten Einkommensnachweis in den Fällen, in denen es für die Gewährung von Leistungen auf die genaue Höhe nicht ankommt, habe ich mich eingesetzt (11. TB S. 53). Die Bundesanstalt für Arbeit hat dafür jetzt eine datenschutzfreundliche Regelung eingeführt; siehe dazu Nr. 12.2 in diesem Bericht.

32. Nach einer Kontrolle einer Verwaltungsgemeinschaft mehrerer Sozialversicherungsträger habe ich dem Bundesminister für Arbeit und Sozialordnung (BMA) empfohlen, die Ergebnisse auch für ähnlich organisierte Sozialversicherungsträger auszuwerten (11. TB S. 57f.). Der BMA ist dieser Empfehlung gefolgt; siehe dazu Nr. 11.5 in diesem Bericht.

33. Zur gesetzlichen Einführung des Sozialversicherungsausweises habe ich Anregungen gegeben (11. TB S. 50f.). Im Gesetzgebungsverfahren konnte eine Reihe von Verbesserungen erreicht werden; siehe dazu Nr. 11.1 in diesem Bericht.

34. Bei der Übersendung von Versicherungsverläufen durch die BfA an ihre Versichertenältesten zum Zwecke der Einzelberatung eines Versicherten habe ich angeregt, diesen stärker in das Verfahren einzubeziehen (11. TB S. 57). Diese datenschutzfreundliche Lösung ist wie erwartet eingeführt worden.

35. Die vom Bundeskriminalamt geplante Dienstanweisung zum Einsatz von Personalcomputern (11. TB S. 63) liegt mir noch nicht vor; zur Datenverarbeitung beim Bundeskriminalamt siehe Nr. 17.4 in diesem Bericht.

36. Eine Einschränkung der Speicherung von „anderen Straftaten" als den spezifischen Staatsschutzdelikten in der von der Abteilung Staatsschutz des BKA geführten Datei APIS habe ich empfohlen (11. TB S. 63f.). Eine Einigung wurde nicht erreicht; siehe dazu Nr. 17.1. in diesem Bericht.

37. Über die — noch unzureichenden — Modifikationen des Verfahrens der Einholung von Polizeiauskünften über Stellenbewerber durch den BGS hatte ich berichtet (11. TB S. 65f.). Die Abstimmung zwischen dem Bund und den Ländern dauert noch an.

38. Bei der Änderung der Verkartungspläne für die Abteilung „Linksextremismus" des BfV habe ich den BMI beraten (11. TB S. 67f.). Inzwischen liegen mir weitere Verkartungspläne des BfV vor, deren datenschutzrechtliche Bewertung noch nicht abgeschlossen ist; siehe auch Nr. 19.3 in diesem Bericht.

39. Die praktische Anwendung neuer Vorschriften für die Einrichtung und Erweiterung von Dateien mit personenbezogenen Daten beim BND wollte ich überprüfen (11. TB S. 69). Eine Kontrolle der Anwendung der Weisung für die Einrichtung personenbezogener Dateien beim BND war mir aus Kapazitätsgründen noch nicht möglich.

40. Über meine Kontrolle beim MAD habe ich berichtet (11. TB S. 70 f.). Die Gespräche mit dem BMVg über die Bewertung und Umsetzung der Ergebnisse sind noch nicht abgeschlossen; siehe dazu Nr. 20.4 in diesem Bericht.

41. Dem BMVg habe ich mehrere Anregungen zur Verbesserung der Sicherheit in WEWIS gegeben (11. TB S. 74 f.). Er ist diesen überwiegend gefolgt.

Bonn, den 14. Februar 1990

Dr. Einwag

Anlage 1 (zu 1.1.5, 1.4, 25)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat bei Stimmenthaltung von Bayern in ihrer Sitzung vom 5./6. April 1989 zur

Neuregelung des Bundesdatenschutzgesetzes

folgende Entschließung gefaßt:

1. Die Datenschutzbeauftragten begrüßen die Beschlüsse des Bundesrates zur Neufassung des Bundesdatenschutzgesetzes. Sie sehen darin eine Bestätigung ihrer bisher dazu vertretenen Meinung und erinnern an ihre Beschlüsse vom 14. März 1986 und vom 6. Juni 1988.

2. Die Datenschutzbeauftragten betonen nochmals die Notwendigkeit,

   — die Datenerhebung im Bundesdatenschutzgesetz zu regeln;

   — die Verarbeitung personenbezogener Daten in Akten in das Bundesdatenschutzgesetz einzubeziehen;

   — die lückenlose Kontrolle durch die Datenschutzbeauftragten zu gewährleisten;

   — im öffentlichen und nicht-öffentlichen Bereich, ungeachtet aller erforderlichen Differenzierung, einen gleichwertigen Datenschutz sicherzustellen.

3. Die Datenschutzbeauftragten weisen schließlich mit Nachdruck darauf hin, daß eine Verabschiedung des Regierungsentwurfs ohne die gebotene Nachbesserung, aber auch eine weitere Verzögerung des Gesetzgebungsvorhabens die Gefahr einer Rechtszersplitterung verstärken würde, die sich schon jetzt deutlich abzeichnet.

Anlage 2 (zu 1.4)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zu den Änderungen des Gesetzes zu Art. 10 GG und der Strafprozeßordnung im Rahmen der Poststrukturreform

Der im Rahmen der Ausschußberatungen zur Poststrukturreform aus den Reihen des Bundestages eingebrachte Entwurf zur Änderung des Gesetzes zu Art. 10 GG (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses) soll die Verfassungsschutzbehörden des Bundes und der Länder, den Militärischen Abschirmdienst und den Bundesnachrichtendienst u. a. dazu ermächtigen, den Fernmeldeverkehr zu überwachen und aufzuzeichnen. Bisher war den Diensten nach dem Gesetz zu Art. 10 GG nur gestattet, „den Fernschreibverkehr mitzulesen, den Fernmeldeverkehr abzuhören und auf Tonträger aufzunehmen". Auch die Überwachungsvorschriften der Strafprozeßordnung (§§ 100a, 100b) sollen entsprechend verändert werden.

Während in der Vergangenheit neben dem Briefverkehr nur Telefongespräche und Fernschreiben kontrolliert und ausgewertet werden durften, soll dies nach dem Entwurf in Zukunft für den gesamten Fernmeldeverkehr (z. B. Btx, Temex, Telefax, Datel-Dienste, ISDN) zulässig sein. Daraus ließe sich ableiten, daß auch Abrechnungs-, Verbindungs- und Nutzungsdaten sowie im Rahmen elektronischer Dienste gespeicherte Inhaltsdaten (z. B. bei Mailboxen, Btx usw.) kontrolliert werden dürfen. Damit würde jedenfalls für den Bereich der Strafprozeßordnung auch eine rückwirkende Kontrolle legalisiert. Nicht auszuschließen ist außerdem, daß Dienstebetreiber dazu verpflichtet werden, für Überwachungszwecke in größerem Umfang Daten zu speichern, als für ihre betrieblichen Belange erforderlich und zulässig ist.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß derart weitgehende Eingriffe in Grundrechte einer gründlichen Prüfung durch alle Beteiligten bedürfen. Deshalb sollten im Rahmen der vom Bundestag als dringlich angesehenen Poststrukturreform das Gesetz zu Art. 10 GG und die Strafprozeßordnung nur insoweit geändert werden, als dies in einem unmittelbaren Zusammenhang zu den geplanten ordnungspolitischen Änderungen der Telekommunikation steht. In Betracht käme insofern lediglich die Einbeziehung der Betreiber privater Telekommunikationsdienste in die Regelungen, die bislang nur für die Post gelten.

Anlage 3 (zu 1.4, 4.1)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts (Strafverfahrensänderungsgesetz vom 3. November 1988)

Die Konferenz begrüßt, daß ein Entwurf zur Regelung des Datenschutzes im Strafverfahrensrecht vorgelegt worden ist und daß darin für die besonderen Ermittlungs- und Fahndungsmethoden eigenständige Befugnisnormen vorgesehen sind sowie Regelungen zur Verarbeitung personenbezogener Daten und zur Akteneinsicht in die Strafprozeßordnung aufgenommen werden sollen.

Die im Entwurf vorgesehenen Datenschutzregelungen sind an den verfassungsrechtlichen Grundsätzen der Verhältnismäßigkeit und Normenklarheit zu messen. Weil im Bereich der Grundrechtsausübung nach der Rechtsprechung des Bundesverfassungsgerichts alle wesentlichen Entscheidungen vom Gesetzgeber selbst zu treffen sind, ist die gesamte Informationsverarbeitung wegen ihres Eingriffscharakters in der Strafprozeßordnung präzise und umfassend gesetzlich zu regeln.

Der vorliegende Entwurf entspricht den sich aus dem Recht auf informelle Selbstbestimmung ergebenden Anforderungen noch nicht; er ist im übrigen unvollständig. Die Datenschutzkonferenz hebt deshalb unter gleichzeitiger Bezugnahme auf ihren Beschluß vom November 1986 folgende Kritikpunkte hervor:

1. *Zu den Regelungen über die Ermittlungs- und Fahndungsmethoden*

— Die Erhebung und Weiterverarbeitung personenbezogener Daten durch Strafverfolgungsorgane greift empfindlich in das Persönlichkeitsrecht der Bürger ein. Umso wichtiger ist es, nach dem Grad der Betroffenheit im Gesetz Abstufungen vorzunehmen. Zwischen dem Beschuldigten, dem Verdächtigen, dem von Vorfeldermittlungen Betroffenen und dem erkennbar nicht Verdächtigen (z. B. Geschädigten, Zeugen) sollte daher unterschieden werden. Vor allem die Regelungen über „Kontakt- und Begleitpersonen", „andere Personen" und „Dritte" werden dem nicht gerecht.

— Es muß klargestellt werden, daß die Ermittlungsgeneralklausel keine Eingriffe gestattet, die in ihrer Eingriffstiefe den besonders geregelten gleichkommen. So wären z. B. die Voraussetzungen des Einsatzes von V-Leuten besonders zu regeln. Auch weiterentwickelte „besondere Fahndungs- und Ermittlungsmethoden" dürfen nicht auf die Ermittlungsgeneralklausel gestützt werden. In die Strafprozeßordnung sind Verfahrensregelungen aufzunehmen, die eine Information etwa der zuständigen Parlamentsausschüsse über die beabsichtigte Anwendung vorsehen. Vor dem Einsatz qualitativ neuer Methoden müssen auf jeden Fall gesetzliche Regelungen geschaffen werden.

— Der Entwurf betont zu recht, daß bei jeder einzelnen Ermittlungs- und Datenverarbeitungsmaßnahme der Grundsatz der Verhältnismäßigkeit zu beachten ist. Dies muß bereits in einzelnen Befugnisnormen zum Ausdruck kommen. Die bislang vorgesehenen Straftatenkataloge sind mit dem Ziel einer Einschränkung zu überprüfen; die bloße Anknüpfung an den Begriff der „Straftat mit erheblicher Bedeutung" ohne weitere Differenzierung reicht nicht aus.

— Die Anordnung von Ermittlungs- und Fahndungsmethoden, die besonders stark in das Recht auf informationelle Selbstbestimmung eingreifen, ist dem Richter vorzubehalten. Gleiches gilt, wenn mit solchen besonderen Methoden erhobene Daten für andere Strafverfahren oder für andere — polizeiliche — Zwecke verwendet werden sollen.

— Wegen der Tiefe der Eingriffe bei besonderen Ermittlungs- und Fahndungsmethoden darf der Richtervorbehalt — von besonderen Eilfällen abgesehen — nicht durch Entscheidungen der Staatsanwaltschaft oder der Polizei ersetzt werden. Soweit ausnahmsweise die Staatsanwaltschaft oder die Polizei eine Anordnung treffen muß, dürfen erlangte Daten nicht weiter verwendet werden, wenn die richterliche Bestägigung ausbleibt; erhobene Daten sind zu löschen.

— Die Verwendung von durch besondere Ermittlungs- oder Fahndungsmethoden erlangten Daten für polizeiliche Zwecke muß neben dem Richtervorbehalt voraussetzen, daß das Polizeirecht vergleichbare Eingriffe gestattet oder daß die Daten zur Abwehr einer gegenwärtigen Gefahr für Leib und Leben erforderlich sind.

2. *Zu den besonderen Regelungen über die Datenverarbeitung*

Regelungen über die Datenverarbeitung im Strafverfahren setzen eine Gesamtkonzeption über die Informationsverarbeitung bei den Strafverfolgungsbehörden voraus. Notwendig sind insbesondere klare Bestimmungen über die Zusammenarbeit zwischen Staatsanwaltschaft und Polizei. Der vorliegende Entwurf läßt den hierzu notwendigen Konsens jedoch nicht erkennen.

— Der Gesetzgeber sollte möglichst genau regeln, welche Arten von Daten für „Zwecke des Strafver-

fahrens", für Zwecke anderer Strafverfahren oder für die Aufklärung künftiger Straftaten in automatisierten Dateien landes- oder bundesweit zur Verfügung stehen sollen und in welchem Verhältnis hierzu das Bundeszentralregister steht.

— Der Gesetzgeber muß, auch um Doppelspeicherungen zwischen staatsanwaltlichen und polizeilichen Informationssystemen zu vermeiden, eindeutig festlegen, wem die Entscheidungsbefugnis über die bei der Strafverfolgung angefallenen Daten zusteht und für welche Zwecke sie verwendet werden dürfen.

— Daten, die für bloße Tätigkeitsnachweise gespeichert werden (Vorgangsverwaltung), dürfen für andere Zwecke nicht verwendet werden und müssen nach kurzen Fristen gelöscht werden.

— Die vorgesehene Speicherung von Daten über Personen, die „bei einer künftigen Strafverfolgung als Zeugen in Betracht kommen", oder die „Opfer einer Straftat werden könnten", gibt zu Bedenken Anlaß, weil das Anlegen von Dateien über besondere Personengruppen wie z. B. Prostituierte, Homosexuelle und ausländische Gastwirte als erlaubt angesehen werden könnte.

— Die Datenspeicherung über Personen, die mangels hinreichendem Tatverdacht freigesprochen worden sind oder bei denen das Ermittlungsverfahren eingestellt oder die Anklage nicht zugelassen worden ist, darf nur unter engeren Voraussetzungen erfolgen.

3. *Zur Akteneinsicht*

Strafakten sind wegen ihres teilweise sehr sensiblen Inhalts geheimzuhalten. Sie dürfen deshalb auch anderen öffentlichen Stellen nur unter engeren Voraussetzungen zugänglich sein. Nicht am Strafverfahren beteiligte Personen dürfen auch über Rechtsanwälte allenfalls in besonderen Ausnahmefällen Einsicht oder Auskunft aus Strafakten erhalten.

4. *Fehlende Regelungen*

Regelungsbedürftig sind außerdem vor allem:

— die engere Festlegung der Zulässigkeit erkennungsdienstlicher Behandlung und der Voraussetzungen für den Fahndungsabgleich sowie die weitere Verwendung der dabei gewonnenen Daten,

— die Verbesserung des Schutzes der Persönlichkeitsrechte bei der Erhebung persönlicher Daten von Angeklagten und Zeugen in Strafverfahren,

— der allenfalls begrenzte Einsatz der Genomanalyse im Strafverfahren.

Anlage 4 (zu 1.4, 14)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 5./6. April 1989 zum Entwurf eines Rentenreformgesetzes 1992

Die Rentenversicherung erfaßt den weit überwiegenden Teil der Bevölkerung mit Daten über das Einkommen sowie über familiäre und gesundheitliche Verhältnisse. Sowohl Pflichtmitglieder als auch freiwillige Versicherte haben nur einen sehr begrenzten Einfluß auf die Erhebung, Speicherung, Verwendung und Weitergabe ihrer Daten. Dies führt zu Eingriffen in das Recht auf informationelle Selbstbestimmung, die einer verfassungsmäßigen gesetzlichen Grundlage bedürfen.

Der Zwang zur Angabe personenbezogener Daten im Rahmen des Versicherungsverhältnisses setzt voraus, daß der Gesetzgeber den Verwendungszweck sowie Art und Umfang der erforderlichen Daten präzise bestimmt. Die Verwendung der Daten ist grundsätzlich auf den gesetzlich bestimmten Zweck zu begrenzen. Bei Anwendung dieser Grundsätze sind zur Verbesserung des Datenschutzes Änderungen oder Ergänzungen des Rentenreformgesetzes notwendig. Dies gilt insbesondere in folgenden Punkten:

1. Für die Erhebung, Verarbeitung und Offenbarung von Versichertendaten, insbesondere von Gesundheitsdaten, bedarf es konkreter Befugnisnormen, die auf die verschiedenen Aufgaben der Rentenversicherungsträger abstellen.
2. Um die zweckgebundene Verwendung der Versichertendaten sicherzustellen, müssen auch die Aufgaben der Rentenversicherung normenklar und übersichtlich im Gesetz dargestellt werden.
3. In das Gesetz sollten Regelungen über Aufbewahrungs- und Löschungsfristen aufgenommen werden.
4. Im Gesetz ist klarzustellen,
   - welche versicherungserheblichen Daten im Versicherungskonto gespeichert werden dürfen;
   - welche Stellen am sog. Rentenauskunftsverfahren teilnehmen und worüber Auskünfte erteilt werden;
   - welche Aufgaben der Deutschen Bundespost im Zusammenhang mit der Rentenversicherung obliegen und welche Datenübermittlungen zwischen Rentenversicherungsträgern, Bundespost und anderen Beteiligten erfolgen;
   - welche Daten in der Zentraldatei bei der Datenstelle der Rentenversicherungsträger (VDR) geführt werden und wer auf diese Daten Zugriff hat.
5. Um für die eigenen Mitarbeiter der Rentenversicherungsträger den Sozial- und Personaldatenschutz zu gewährleisten, sollte die organisatorische und personelle Trennung der Sachbearbeitung von der Personaldatenverarbeitung vorgeschrieben werden.
6. Eine eindeutige Klarstellung der Rechtsaufsicht und der Datenschutzkontrolle über die Datenstelle der Rentenversicherungsträger ist erforderlich.

Anlage 5 (zu 1.1.5, 1.4)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz zu den Entwürfen eines Bundesverfassungsschutzgesetzes (BVerfSchG), eines MAD-Gesetzes (MADG) und eines BND-Gesetzes (BNDG) vom 30. Mai 1989

I.

Mit den von der Bundesregierung vorgelegten Entwürfen sollen die nach der Rechtsprechung des Bundesverfassungsgerichts erforderlichen bereichspezifischen Rechtsgrundlagen für die Informationsverarbeitung der Verfassungsschutzbehörden und Nachrichtendienste geschaffen werden. So dringend die Beseitigung der bestehenden Regelungsdefizite auch ist, müssen sich neue Gesetze gerade in diesem Bereich in besonderem Maße daran messen lassen, daß in die Freiheitsrechte der Bürger nicht unverhältnismäßig eingegriffen wird. Dieser Vorgabe werden auch die nunmehr vorgelegten Entwürfe in vielerlei Hinsicht nicht gerecht.

II.

1. Da sich der zulässige Umfang der Informationsverarbeitung nach den Aufgaben der datenverarbeitenden Stelle bemißt, bedarf es einer abschließenden, möglichst genauen gesetzlichen Beschreibung dieser Aufgaben. Für den einzelnen muß erkennbar sein, wann er die Schwelle von der Ausübung der Grundrechte zur verfassungsfeindlichen Bestrebung überschreitet. Die in § 3 Abs. 1 verwendeten Begriffe, wie etwa „Bestrebungen gegen die freiheitliche demokratische Grundordnung" oder „Gefährdung auswärtiger Belange" stellen dies nicht sicher. Insbesondere bleibt unklar,

   — ob der Begriff der Bestrebungen das Handeln einer Mehrzahl von Personen in einem gewissen Grad von Organisiertheit voraussetzt oder auch das Tätigwerden einer einzelnen Person beinhaltet;

   — ob es zulässig sein soll, Informationen auch über solche Bestrebungen zu sammeln und zu speichern, die erkennbar nicht gegen die freiheitliche demokratische Grundordnung gerichtet sind, an denen aber Personen beteiligt sind, die an anderen gegen diese Grundordnung gerichteten Bestrebungen mitwirken;

   — ob und ggf. in welchem Umfang Informationen über nicht extremistische Organisationen gesammelt und gespeichert werden dürfen, die Gegenstand extremistischer Beeinflussung (-sversuche) sind.

   Zur weiteren Umschreibung der Aufgaben könnte auch der Inhalt von § 92 StGB mit herangezogen werden.

2. Bei einer derartig vagen Umschreibung der Aufgaben wäre es um so notwendiger, die Voraussetzungen für die Erhebung, Speicherung und sonstige Verwendung personenbezogener Daten je nach dem, welche seiner ganz unterschiedlichen Aufgaben (Spionageabwehr, Extremismus- und Terrorismusbeobachtung, Sicherheitsüberprüfung) der Verfassungsschutz wahrnimmt, differenziert, präzise und für den Bürger transparent zu regeln. Stattdessen sieht der Entwurf pauschale Befugnisse für den Verfassungsschutz vor. Außerdem fehlen Regelungen darüber, ob und ggf. in welchem Umfang, für welche Zwecke und mit welchen Speicherungsfristen Daten über unverdächtige und unbeteiligte Personen erhoben und gespeichert werden dürfen.

3. Unklar ist, welche rechtlichen Grenzen dem Einsatz nachrichtendienstlicher Mittel gesetzt sind. Außerdem muß klargestellt werden, daß die Befugnis zum Einsatz nachrichtendienstlicher Mittel kein genereller Rechtfertigungsgrund für Verstöße gegen Straftatbestände ist, gegen wen sich der Einsatz nachrichtendienstlicher Mittel richten darf und was mit den ggf. dabei über Unverdächtige gewonnenen Daten geschehen darf. Auch im übrigen sollten beim Einsatz nachrichtendienstlicher Mittel, die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen, entsprechende Schutzrechte wie im Gesetz zu Art. 10 Grundgesetz vorgesehen werden (z. B. Verwertungsverbot, Unterrichtungen).

4. Der Entwurf regelt im wesentlichen lediglich die Speicherung personenbezogener Daten in Dateien, obwohl die Informationstechnik es schon heute ermöglicht, auch komplexe Datensammlungen — bestehend aus Akten, Dateien und anderen Unterlagen — gezielt mit Hilfe automatischer Verfahren zu erschließen.

5. Bei der Regelung insbesondere für die gemeinsamen Verbunddateien der Verfassungsschutzbehörden sollte auch klargestellt werden, daß in Textdateien nur Daten über solche Personen gespeichert werden dürfen, die selbst in Verdacht stehen, eine der im Gesetzentwurf aufgezählten Straftaten zu planen, zu begehen oder begangen zu haben. Darüber hinaus ist sicherzustellen, daß in der Datei die für die Bewertung und Überprüfung von Textzusätzen maßgeblichen Unterlagen angegeben werden.

6. Die Frage, ob Einsicht in amtliche Register zulässig sein soll, kann nur bereichsspezifisch geregelt werden. Die Zulässigkeit der Einsichtnahme in Register rechtfertigt nicht die Einrichtung von online-Anschlüssen.

7. Das Zweckbindungsgebot ist sowohl für Übermittlungen an den Verfassungsschutz als auch für solche durch den Verfassungsschutz nicht ausreichend berücksichtigt. Die nunmehr vorgesehenen Übermittlungseinschränkungen reichen vor allem deshalb nicht aus, weil die übermittelnde Stelle nicht ausdrücklich verpflichtet wird zu prüfen, ob schutzwürdige Belange entgegenstehen. Auch innerhalb des Bundesamtes für Verfassungsschutz darf nicht jede Information unabhängig von ihrer Herkunft für jede Aufgabe verwendet werden.

8. Aus dem Trennungsgebot für Polizei- und Nachrichtendienste folgt insbesondere, daß die Übermittlung von Daten, die die Polizei unter Einsatz dem Verfassungsschutz vorenthaltener Befugnisse, z. B. bei Hausdurchsuchungen, gewonnen hat, nur nach Maßgabe einschränkender Verwertungsregelungen erfolgen darf. Die Ansatzpunkte, die im Entwurf der letzten Legislaturperiode enthalten waren, sollten wieder aufgegriffen werden.

   Die Informationshilfe der Grenzpolizeien für den Verfassungsschutz muß einschränkend geregelt werden.

9. Es fehlen auch befriedigende Löschungsregelungen. Abgesehen davon, daß die Löschung von Daten in Akten nicht einmal erwähnt wird, sollten schon im Gesetz Regelfristen für die Überprüfung und Löschung der verarbeiteten Daten festgelegt werden. Dabei sollte zwischen den einzelnen Aufgabenbereichen des Bundesamtes für Verfassungsschutz unterschieden werden.

10. Die Einschränkungen des Auskunftsrechts der Bürger sind bereichsspezifisch im Bundesverfassungsschutzgesetz zu regeln. Ein Auskunftsanspruch besteht in der Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht. Im übrigen bedarf es einer Abwägung im Einzelfall. Die Ablehnung ist gegenüber dem Betroffenen soweit zu begründen, daß er sachgerecht darüber entscheiden kann, ob und welche Rechtsmittel er einlegen will. Außerdem ist der Betroffene auf sein Recht hinzuweisen, sich an den Datenschutzbeauftragten zu wenden.

11. Die Datenschutzbeauftragten begrüßen es, daß die Beteiligung des Verfassungsschutzes an Sicherheitsüberprüfungen und Überprüfungen im Rahmen des vorbeugenden personellen Sabotageschutzes in einem eigenen Geheimschutzgesetz geregelt werden sollen. Sofern über die Sicherheitsüberprüfung hinaus eine Mitwirkung an anderen Verfahren für unabdingbar gehalten wird, sind diese gesetzlich zu regeln.

12. Soweit die Entwürfe für ein MAD-Gesetz und ein BND-Gesetz auf das Bundesverfassungsschutzgesetz verweisen, gilt die hierzu geäußerte Kritik. Die in den Entwürfen vorgesehene Verweisungstechnik erhöht für den Bürger die Schwierigkeit, aus den Gesetzen klar zu erkennen, welche personenbezogenen Daten die Dienste bei welcher Gelegenheit über ihn verarbeiten dürfen. Darüber hinaus bestehen Zweifel, ob die für das Bundesamt für Verfassungsschutz vorgesehenen Befugnisse pauschal auch für den Militärischen Abschirmdienst notwendig sind, der als Teil der Streitkräfte ein gegenüber dem Bundesamt für Verfassungsschutz deutlich unterschiedliches Operationsgebiet hat.

Anlage 6 (zu 1.1.3, 1.4, 27.6)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 1989 zum

Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen

1. Am 14. Juni 1985 unterzeichneten die Regierungen Frankreichs, der Bundesrepublik Deutschland und der Beneluxstaaten in Schengen/Luxemburg ein Abkommen über den schrittweisen Abbau der Grenzen zwischen ihren Ländern. Dabei knüpften sie den Wegfall der Grenzkontrollen an eine Reihe von Maßnahmen, die die befürchteten Sicherheitsdefizite ausgleichen sollen. Die Maßnahmen sollen in einem Zusatzübereinkommen festgehalten werden. Hierzu gehört die Errichtung eines gemeinsamen automatisierten Informationssystems für den Bereich der Fahndung (Schengener Informationssystem — SIS). Dieses System dient vor allem der Ausschreibung zur Festnahme und zur Zurückweisung an der Grenze, der verdeckten Registrierung und der Ermittlung des Aufenthalts von Zeugen im Strafverfahren. Überdies sollen der Informationsaustausch zum Zwecke der Bekämpfung bestimmter Formen der Kriminalität verstärkt, die ausländer- und asylrechtlichen Entscheidungen vereinheitlicht und ein gemeinsames Verfahren für intensivierte Kontrollen an den Außengrenzen festgelegt werden.

2. Die Vertragsstaaten verpflichten sich in dem Entwurf zum Zusatzübereinkommen, Datenschutzvorschriften für das Schengener Informationssystem entsprechend den Grundsätzen der Datenschutzkonvention des Europarates und der Empfehlung des Ministerkomitees des Europarats an die Mitgliedsstaaten über die Nutzung personenbezogener Daten im Polizeibereich als Mindeststandard zu erlassen. Die Konferenz begrüßt dies und stellt zugleich fest, daß nach dem gegenwärtigen Stand der Verhandlungen auch die in der Erklärung der Datenschutzorgane Frankreichs, Luxemburgs und der Bundesrepublik Deutschland vom 16. März 1989 enthaltenen Forderungen in wesentlichen Bereichen erfüllt werden sollen. Der Vertragsentwurf sieht für das Schengener Informationssystem vor: Auskunfts-, Berichtigungs- und Klagerechte für die Betroffenen; Kontrollorgane auf nationaler und internationaler Ebene; eine Zweckbindung der Daten. Diese Elemente müssen Bestandteile des Zusatzübereinkommens bleiben, bedürfen aber noch der Verbesserung und Ergänzung, damit sich durch den grenzüberschreitenden Datenaustausch keine gravierenden Verschlechterungen für den Datenschutz ergeben.

2.1 Die Datenschutzbeauftragten fordern für das SIS insbesondere die

- Festlegung der Voraussetzungen, nach denen unter Berücksichtigung der Verhältnismäßigkeit (zum Beispiel nach der Schwere der Straftaten) Informationen aus dem nationalen in den internationalen Fahndungsbestand übernommen werden sollen,
- Festlegung, unter welchen Voraussetzungen und in welchem Umfang die verschiedenen Inlandsbehörden auf die Daten zugreifen dürfen,
- konkrete Beschreibung der Voraussetzungen, unter denen verdeckte Registrierungen erlaubt werden sollen (Straftatenkatalog),
- präzisere Beschreibung der Kriterien, nach denen Zweckdurchbrechungen zur Verhütung einer Straftat mit erheblicher Bedeutung sowie aus schwerwiegenden Gründen der Staatssicherheit erlaubt werden sollen, und
- Aufnahme einer Verpflichtung, Zweckänderungen zu Kontrollzwecken zu dokumentieren.

2.2 Die Regelungen über den Datenschutz — insbesondere die Rechte der Betroffenen und die Datenschutzkontrolle — müssen auf die im Zusatzübereinkommen vorgesehene konventionelle Verarbeitung personenbezogener Daten ausgedehnt werden. Dies gilt vor allem für den Informationsaustausch in den Bereichen des Ausländerrechts und des Asylverfahrens.

3. Der Entwurf des Zusatzübereinkommens enthält eine pauschale Verpflichtung der Vertragsparteien, daß ihre nationalen Sicherheitsdienste sich untereinander unter Berücksichtigung des nationalen Rechts und nach Maßgabe ihrer jeweiligen Zuständigkeit bei der Abwehr von Nachteilen für die Staatssicherheit Hilfe leisten.

   Die Datenschutzbeauftragten weisen vorsorglich darauf hin, daß eine solche Bestimmung nach deutschem Verfassungsrecht keine tragfähige Grundlage für einen umfassenden Datenaustausch der Geheimdienste darstellt.

4. Der Vertragsentwurf verpflichtet jeden Vertragsstaat, Ausländer aus dritten Staaten an der Grenze zurückzuweisen, wenn ein anderer Vertragsstaat ihn „zur Einreiseverweigerung" ausgeschrieben hat. Es ist nicht vorgesehen, daß der vollziehende Staat die Gründe der Ausschreibung zur Kenntnis nimmt und rechtlich überprüft. Die Datenschutz-

beauftragten fordern die verbindliche Festlegung der sachlichen Voraussetzungen solcher Ausschreibungen und die Ermöglichung einer Überprüfung.

5. Die Datenschutzbeauftragten machen darauf aufmerksam, daß das Zusatzübereinkommen den deutschen Gesetzgeber nicht von der dringenden Notwendigkeit enthebt, vor Inkrafttreten des Zusatzübereinkommens für die polizeiliche Datenverarbeitung verfassungskonforme Rechtsgrundlagen zu schaffen.

6. Bevor die einzelnen Vertragsstaaten ihre im Entwurf des Zusatzübereinkommens vorgesehene Verpflichtung, spezielle nationale Regelungen für das Erheben und Nutzen von Daten zu erlassen, nicht erfüllt haben, dürfen Daten an diese Staaten auf der Grundlage des Zusatzübereinkommens nicht übermittelt werden.

Anlage 7 (zu 1.4, 10.3)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. 10. 1989 über

Genomanalyse und informationelle Selbstbestimmung

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz hat den Abschlußbericht der Enquête-Kommission des Deutschen Bundestages „Chancen und Risiken der Gentechnologie" (Drucksache 10/6775) zum Anlaß genommen, die Risiken für die informationelle Selbstbestimmung jedes Betroffenen abzuwägen gegenüber den Chancen, die die Genomanalyse bringt. Durch die Offenlegung genetischer Daten eines Menschen kann dieser in seinem Persönlichkeitsrecht und sonstigen schutzwürdigen Belangen nachhaltig beeinträchtigt werden. Informationen aus dem Kernbereich der Privatsphäre, die dem Betroffenen selbst bisher unbekannt waren, können ihn zu einem an sich ungewollten Verhalten in seiner Lebens- oder Berufsgestaltung veranlassen; ihre Kenntnis kann zu einer psychischen und sozialen Zwangslage für den Betroffenen führen. Wegen der genetischen Bedingtheit solcher Informationen können sich daher auch entsprechende Auswirkungen auf dritte Personen, insbesondere die Familie, ergeben. Das Bekanntwerden solcher Informationen kann den Betroffenen in seinem sozialen Umfeld diskriminieren mit der möglichen Folge gesellschaftlicher Ausgrenzung.

Um den besonderen Risiken bei der Anwendung der Genomanalyse zu begegnen, bedarf es der gesetzlichen Absicherung folgender Grundsätze:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muß sich auch auf die weitere Verwendung der genetischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnenen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muß zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschußinformationen bringt. Überschußinformationen sind unverzüglich zu vernichten.
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muß auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschußinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, daß genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.
7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.
8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, daß ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muß vermieden werden.

   Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muß berücksichtigt werden.

Die Konferenz versteht ihre Stellungnahme als Beitrag zur Diskussion mit allen Institutionen, die an den Fragen der Genomanalyse arbeiten. Sie legt Wert darauf, den Dialog mit der Wissenschaft fortzusetzen und dabei neue wissenschaftliche Erkenntnisse einzubeziehen.

Anlage 8 (zu 1.1.3, 1.4, 27.3)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 1989 über den

Datenschutz in der Europäischen Gemeinschaft

Angesichts der für das Jahr 1993 zu erwartenden Errichtung eines Binnenmarktes in der Europäischen Gemeinschaft zählt der grenzüberschreitende Datenaustausch zu den drängenden, ungelösten Problemen des Datenschutzes.

Eine internationale Datenverarbeitung ist nicht nur eine Grundbedingung für eine gemeinschaftsweite privatwirtschaftliche Tätigkeit. Auch für den öffentlichen Bereich gewinnt die Problematik zunehmend an Bedeutung. Der Abbau der Grenzkontrollen in der Europäischen Gemeinschaft und das vor diesem Hintergrund geschlossene „Schengener Übereinkommen" über die verstärkte informationelle Zusammenarbeit der Polizeibehörden Frankreichs, der Bundesrepublik Deutschland und der Benelux-Staaten sind dafür ein signifikantes Beispiel.

Ebenso werden die technischen Voraussetzungen für internationale Datenübermittlungen immer weiter verbessert. Schon 1993 soll europaweit das digitale, diensteintegrierende Kommunikationsnetz (ISDN) zur Verfügung stehen.

In der Europäischen Gemeinschaft wird die Dynamik der wirtschaftlichen Integration die Entwicklung zu einem „informationellen Großraum" nachhaltig fördern. Dies hat zur Folge, daß die Informationsverarbeitung insbesondere in den Bereichen Umweltschutz, Forschung, Arbeitsmarkt, soziale Sicherung, Statistik und öffentliche Sicherheit erheblich zunehmen wird.

Die Beratungen der Internationalen Konferenz der Datenschutzbeauftragten im August 1989 in Berlin haben erneut gezeigt, daß die auf supranationaler Ebene vorhandenen Regelungen, wie etwa die Europaratskonvention von 1981, zwar wichtige Prinzipien für einen fairen Datenumgang enthalten, aber keineswegs ausreichen, den etwa in der Bundesrepublik Deutschland oder Frankreich durch das nationale Datenschutzrecht erreichten Stand der Sicherung des informationellen Selbstbestimmungsrechts des Bürgers zu gewährleisten, abgesehen davon, daß eine Reihe von Mitgliedsstaaten der Gemeinschaft die Konvention noch nicht ratifiziert hat.

Besonders bedenklich ist die Untätigkeit der EG im Bereich des Datenschutzes. Rechtsakte der EG verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung, Verarbeitung und Übermittlung personenbezogener Daten, etwa im Bereich der Statistik. Die Telekommunikationspolitik der EG ist auf einen forcierten Ausbau europaweit standardisierter und operierender Telekommunikationsdienste und -netze gerichtet. Zwischen den verschiedenen nationalen Datenschutzrechten der Mitgliedstaaten bestehen im Hinblick auf Verarbeitungsvoraussetzungen, Rechte der betroffenen Personen und Kontrollmöglichkeiten große Unterschiede.

Die Konferenz bekräftigt daher die auf der Internationalen Konferenz in Berlin einmütig erhobenen Forderungen,

— daß bei der Entwicklung und Nutzung grenzüberschreitender Datennetze und Datendienste dem Datenschutz der gleiche Stellenwert zukommen muß, wie der Förderung der technischen Infrastruktur,

— daß die EG ein Gesamtkonzept für die Sicherung des Datenschutzes sowohl in den Mitgliedsländern als auch bei ihren eigenen Aktivitäten entwickeln muß, das insbesondere die Gleichwertigkeit des Schutzniveaus in der gesamten Gemeinschaft herstellt, und

— daß auf der EG-Ebene eine unabhängige Datenschutzinstanz einzurichten ist, die die Institution der Gemeinschaft in allen Datenschutzfragen berät, die Verarbeitung personenbezogener Daten durch die EG-Gremien überwacht, Eingaben von Bürgern entgegennimmt und mit den nationalen Datenschutzorganen zusammenarbeitet.

Die Konferenz der Datenschutzbeauftragten erklärt ihre ausdrückliche Bereitschaft, ihre Kenntnisse und Erfahrungen bei der Realisierung dieser Maßnahmen einzubringen. Ansprechpartner sind dabei zum einen die Organe der Gemeinschaft, insbesondere das Europäische Parlament, zum anderen die an der Willensbildung der EG beteiligten deutschen Behörden des Bundes und der Länder.

Anlage 9 (zu 1.1.3, 1.4, 27.3)

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26./27. Oktober 1989 zum

Entwurf einer EG-Statistikverordnung

Die Kommission der Europäischen Gemeinschaften hat den Entwurf einer Verordnung des Rates über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften vorgelegt.

Diese Verordnung darf nicht hinter dem datenschutzrechtlichen Standard der amtlichen Statistik in der Bundesrepublik Deutschland zurückbleiben.

Die nationalen Statistikämter sollen nach dem Vorschlag der EG-Kommission die Befugnis erhalten, vertrauliche statistische Daten dem Statistischen Amt der Europäischen Gemeinschaften auch dann zu übermitteln, wenn sie einen Personenbezug aufweisen. Es ist nicht auszuschließen, daß auf nationaler Ebene kurzfristig für bestimmte statistische Zwecke vorgehaltene personenbezogene Datenbestände (z. B. noch nicht anonymisierte Daten aus dem Mikrozensus) durch das Statistische Amt der EG abgerufen werden. Deshalb muß in der EG-Verordnung festgelegt werden, daß die Übermittlung personenbezogener Einzelangaben nur ausnahmsweise durch einen weiteren Rechtsakt der EG für bestimmte statistische Zwecke (z. B. für die Produktions-, Industrie- und Außenhandelsstatistik) zugelassen werden darf und daß eine möglichst frühzeitige Anonymisierung stattfindet sowie notwendige organisatorisch-technische Maßnahmen der Datensicherung getroffen werden.

Die unabhängige Datenschutzkontrolle auf Gemeinschaftsebene ist bisher nicht gewährleistet. Der geplante Beratende Ausschuß kann diese Kontrolle nicht ersetzen.

Im Gemeinschaftsrecht sind bisher für die Verletzung des Statistikgeheimnisses keine ausreichenden Sanktionen vorgesehen. Nicht einmal alle Mitgliedsstaaten stellen einen derartigen Verstoß unter Strafe.

Die Teilnehmer der 11. Internationalen Konferenz der Datenschutzbeauftragten in Berlin haben am 30. August 1989 diesen Fragenkreis diskutiert und sind übereingekommen, sich auf nationaler und internationaler Ebene für eine stärkere Berücksichtigung datenschutzrechtlicher Belange im Verordnungsentwurf einzusetzen.

Die Konferenz der Datenschutzbeauftragten appelliert daher an die Bundesregierung und den Ministerrat, vor einer Verabschiedung des Verordnungsentwurfs die aufgezeigten Mängel zu beseitigen, damit den Persönlichkeitsrechten der Gemeinschaftsbürger auch bei der ständig zunehmenden Zahl europäischer Statistiken und bei der für 1990 in den meisten anderen EG-Mitgliedsstaaten vorgesehenen Volkszählung Rechnung getragen wird.

Anlage 10 (zu 16.1)

Statement für die 4. Große Krebskonferenz am 5. Dezember 1989 in Bonn

Von den wichtigen Aufgaben der Krebskonferenz ist die Einrichtung von Krebsregistern, mit denen sich die Arbeitsgruppe Epidemiologie befaßt hat, für den Datenschutz von wesentlicher Bedeutung. In ihrem Votum vom April dieses Jahres hat die Arbeitsgruppe die Gründe für ein Krebsregister dargelegt und gleichzeitig ein Konzept für ein regionales Krebsregister vorgestellt. Hiervon gehe ich aus.

I. Ob Krebsregister und in welcher Struktur notwendig sind, ob es genügt, wenn nur ein Teil der Bevölkerung davon betreut wird oder ob die Erfassung der Gesamtbevölkerung erforderlich ist, ist eine fachliche Frage, bei der Wissenschaftlern und Ärzten das entscheidende Urteil überlassen bleiben muß.

II. Es ist auch Aufgabe der Wissenschaftler und Ärzte, die Anforderungen an Krebsregister zu formulieren. Dabei ist es allerdings notwendig, daß nach gewonnenen Erfahrungen eine reelle Chance für die Realisierung des Konzepts besteht. Ein Konzept für Krebsregister muß daher auf seine Schlüssigkeit, Plausibilität und Realisierbarkeit geprüft werden. Aus den Erfahrungen, die inzwischen mit der Feldstudie in Baden-Württemberg im Zusammenhang mit dem dortigen Verschlüsselungsmodell gewonnen worden sind (vgl. hierzu die Veröffentlichung des Ministeriums für Arbeit, Gesundheit, Familie und Sozialordnung Baden-Württemberg vom Juli 1989), ergeben sich unter diesen Gesichtspunkten Fragen:

1. Nach dem Votum der Arbeitsgruppe Epidemiologie ist eine Vollerfassung aller Erkrankungsfälle notwendig; andererseits soll — sicher zutreffend — von einer Meldepflicht abgesehen werden. Nach der Untersuchung in Baden-Württemberg wollen sich aber 8,3 % der Ärzte in keinem Fall an irgendeinem Krebsregistermodell beteiligen (vgl. S. 27 der o. a. Veröffentlichung). Welchen Einfluß hat dies auf das Modell?

2. Die Notwendigkeit der Vollerfassung wird insbesondere damit begründet, Veränderungen auch bei seltenen Tumoren zu erkennen. Genügt es dann nicht, die Vollerfassung auf diese seltenen Tumore zu beschränken?

3. Wichtige Länder, wie z. B. Bayern, setzen auf den Ausbau klinikbezogener Krebsregister. Können, wenn diese Haltung nicht überwunden werden kann, die angestrebten Ziele noch erreicht werden?

4. An einem Konzept eines Registers ohne Verschlüsselung und ohne Einwilligung wollen sich nach einer Umfrage in Baden-Württemberg nur 11,5 % der Ärzte beteiligen. Da es auf die Bereitschaft der Ärzte zur Beteiligung entscheidend ankommt, spricht viel dafür, daß ein Modell auf dieser Basis nicht die gewünschten und benötigten Erkenntnisse liefert. Die Akzeptanz der Modelle mit Einwilligung des Patienten oder mit Verschlüsselung ist fünf- bis sechsmal höher (vgl. S. 27 der o. a. Veröffentlichung). Ist damit nicht von vornherein der zu beschreitende Weg vorgezeichnet?

5. Die Ergebnisse der Feldstudie in Baden-Württemberg sprechen dafür, daß eine namentliche Meldung des Patienten an das Krebsregister und dessen namentliche Speicherung nicht erforderlich sind. Sollten etwaige Probleme nicht besser durch eine angemessene Fortentwicklung des Verschlüsselungsmodells gelöst werden?

6. Baden-württembergische Ärzte schätzen den Anteil der Patienten, die sie über ihre Krebserkrankung aufklären, und deshalb auch nur um Einwilligung zur Meldung an das Krebsregister bitten können, auf nur 46 %. Sie sind der Meinung, daß von diesen auch nur die Hälfte einer Meldung an das Krebsregister zustimmt. Ist nicht allein dadurch das Verschlüsselungsmodell, bei dem es auf die Einwilligung nicht ankommt, von vornherein überlegen?

7. Die Meldung durch pathologische Institute ist von hoher Bedeutung (bei dem Feldversuch in Baden-Württemberg kamen 47 % der Meldungen von dort). Die Einwilligung des Betroffenen einzuholen, wirft bei solchen Instituten besondere Probleme auf. Meldungen durch Institute ohne Einwilligung des Patienten sind bei Verschlüsselung erheblich leichter zu rechtfertigen. Verlangt nicht diese Ausgangslage ebenfalls das Verschlüsselungsmodell?

Wenn — was von Fachleuten zu beurteilen ist — Krebsregister notwendig sind und nur bei Vollerfassung aller Erkrankungen ihre Aufgabe erfüllen können, hat ein Verschlüsselungsmodell sowohl in bezug auf die Qualität der Meldungen als auch unter datenschutzrechtlichen Gesichtspunkten erhebliche Vorteile. Das in Baden-Württemberg praktizierte Modell sollte deshalb auf der Grundlage des inzwischen vorliegenden Erfahrungsberichts auf seine Eignung für die verfolgten Ziele geprüft werden. Sollte sich dabei die Notwendigkeit zu Verbesserungen ergeben, so kann dieses Konzept sicher auch noch fortentwickelt werden.

Anlage 11 (zu 24.2.3)

Behörde
Organisationseinheit

APC-Verzeichnis

Standort des Geräts
zuständiger Systemverwalter
Hersteller
Modell
Nummer des Geräts
Betriebsystem(e)
benutzte Datenträger
Datenträgerverzeichnis geführt von (Name)

Anschluß an Datennetz(e)?

☐ Nein ☐ Ja, und zwar an — Datennetz(e)

Personenbezogene Daten?

☐ Nein ☐ Ja, zur Übersicht gemeldet am — Datum

Besondere Sicherheitsmaßnahmen? (siehe auch Rückseite)

☐ Nicht erforderlich ☐ Erforderlich, und zwar — Maßnahme

Eintragungen und Sicherungsmaßnahmen zuletzt geprüft

am (Datum)	durch (Unterschrift)
am (Datum)	durch (Unterschrift)
am (Datum)	durch (Unterschrift)
am (Datum)	durch (Unterschrift)
am (Datum)	durch (Unterschrift)
am (Datum)	durch (Unterschrift)

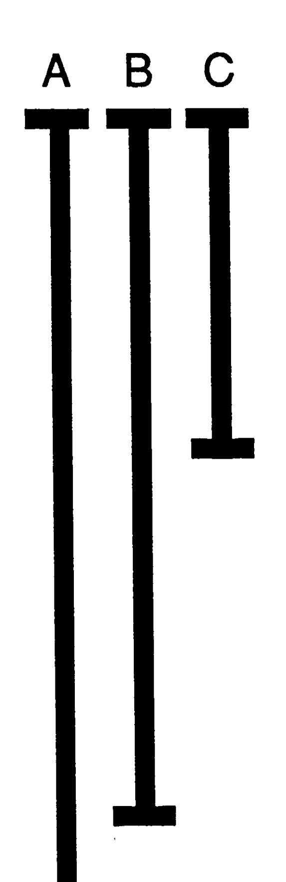
bitte wenden !

Empfehlungen des Bundesbeauftragten für den Datenschutz (BfD) für den Einsatz von Arbeitsplatzcomputern (APC)

A = APC mit Personaldaten oder anderen sensiblen personenbezogenen Daten

B = APC mit sonstigen personenbezogenen Daten

C = alle anderen APC



- keine privaten Geräte
- keine privaten Datenträger
- keine private Software
- Verzeichnis aller Geräte **(siehe Rückseite)**
- Kennzeichnung und Registrierung aller Datenträger **(siehe Verzeichnis der Datenträger)**
- Zugangssicherung

- Systemverwalter (der nicht Nutzer ist)
- sichere Menüführung
- Benutzeranmeldung (mit Paßwort)
- Protokolldatei (die nicht zur Verhaltens- und Leistungskontrolle geeignet ist)

- kryptografische Verschlüsselung
- keine freie Abfragesprache

Personenbezogene Daten sind Angaben, die einer bestimmten oder bestimmbaren Einzelperson zugeordnet werden können. Dies sind also nicht nur Name und Anschrift, sonder z. B. auch Telefonnummer, Raumnummer, Dienststellung, Kraftfahrzeugkennzeichen,Urlaubszeiten

bitte wenden !

Behörde

Organisationseinheit

Stand

Stand

Stand

Stand

Verzeichnis der Datenträger für Gerät-Nummer

Gerät-Nummer

Nummer des Datenträgers *)	Art des Datenträgers	a) beschafft durch b) erhalten von	Standort/Verbleib

*) Jeder Datenträger ist mit seiner Nummer zu kennzeichnen

Anlage 12 (zu 1.1.3, 27.1)

Berliner Resolution der Internationalen Konferenz der Datenschutzbeauftragten vom 30. August 1989

Die Telekommunikation befindet sich weltweit in einer raschen Entwicklung. Über internationale Datennetze werden in wachsendem Umfang auch personenbezogene Daten transferiert, etwa im Zusammenhang mit der Verwendung von Kreditkarten, bei Reise-Buchungs-Systemen und innerhalb multinationaler Unternehmen. Die Nutzung dieser Technologie kann bedeutende Vorteile mit sich bringen. Aber zugleich wird es schwieriger, die Rechte derer zu schützen, deren persönliche Daten rund um die Welt übermittelt werden.

Der Europarat, die OECD, die Vereinten Nationen und weitere internationale Organisationen haben Empfehlungen und Leitlinien zum Datenschutz verabschiedet. Sie enthalten einen gemeinsamen Bestand von Grundsätzen für eine faire Praxis, wie sie etwa in der Konvention des Europarats (Konvention No. 108) und in den OECD-Leitlinien zum Ausdruck kommen. Sie bezwecken den Schutz der Privatheit des einzelnen.

Bisher haben sich acht Staaten durch Beitritt zur Konvention des Europarats international verpflichtet, einen bestimmten Datenschutzstandard einzuhalten. Die Datenschutz-Kontrollinstanzen dieser Länder haben in gewissem Umfang die Befugnis, den grenzüberschreitenden Datenfluß zu kontrollieren, wenn dies zum Schutz einzelner nötig ist. Bei dieser Kontrolle ergeben sich allerdings schwerwiegende praktische Probleme. Datenübermittlung ins Ausland bedeutet deshalb für den einzelnen in der Mehrzahl der Fälle, daß er nicht mehr die Gewißheit haben kann, daß die Grundsätze, die in nationalen Gesetzen und in den verschiedenen internationalen Übereinkommen festgelegt sind, auf seine oder ihre Daten angewandt werden. Zum Beispiel kann es dann keine Garantie geben, daß die Daten auf dem neuesten Stand und genau sind und nur für bestimmte Zwecke verwendet werden. Der einzelne kann auch sein Recht, einen Datenschutzbeauftragten anzurufen, nicht wahrnehmen.

Das Problem eines wirksamen internationalen Datenschutzes läßt sich nur durch gleichwertige gesetzliche Sicherungen in den übermittelnden und empfangenden Ländern lösen. Diese Lösung wird auch von den oben genannten Empfehlungen und Leitlinien vorgezeichnet.

Nach Auffassung der Datenschutzbeauftragten muß bei der Entwicklung und Nutzung internationaler Datendienste dem Datenschutz die gleiche Priorität gegeben werden, wie der Förderung der Datenverarbeitung und der Telekommunikation. Sie empfehlen deshalb:

— Die Regierungen sollten sowohl einzeln als auch im Rahmen internationaler Organisationen darauf hinarbeiten, daß sobald wie möglich gleichwertige gesetzliche Sicherungen geschaffen werden.

— Wer personenbezogene Daten über die Grenzen vermittelt, muß den Schutz beim Empfänger prüfen, damit die Beachtung der Rechte der Betroffenen tatsächlich sichergestellt wird.

Das Ziel dieser Maßnahmen muß sein:

— Die Datenschutzgrundsätze der Konvention 108 und der OECD-Leitlinien werden unabhängig von einer grenzüberschreitenden Übermittlung gewährleistet;

— international operierende Datenverarbeitungssysteme müssen so aufgebaut sein, daß der einzelne ohne unzumutbare Schwierigkeiten seine Datenschutzrechte wahrnehmen kann;

— Berichtigungen, Aktualisierungen und Löschungen von Daten müssen auch im Ausland nachvollzogen werden, wenn die Daten zuvor dorthin übermittelt worden sind;

— die durch den internationalen Datenaustausch erhöhten Gefahren für das Recht der einzelnen, über die Verwendung ihrer Daten zu bestimmen, müssen durch internationale Zusammenarbeit der Datenschutzbeauftragten ausgeglichen werden.

Zusatzerklärung der Datenschutzbeauftragten der EG-Länder

Die Datenschutzbeauftragten der Länder der Europäischen Gemeinschaft sind der Überzeugung, daß die Existenz und die Aktivitäten der Gemeinschaft einerseits besondere Vorkehrungen des Datenschutzes erforderlich machen, andererseits aber auch verbesserte Möglichkeiten bieten, den Datenschutz über nationale Grenzen hinaus wirksam zu machen.

— Der für Ende 1992 angestrebte EG-Binnenmarkt ist auf den freien Austausch von auch personenbezogenen Informationen gerichtet, etwa in den Bereichen Direktmarketing/Adressenhandel und Kreditinformation.

— Entscheidungen der Europäischen Gemeinschaften verpflichten in zunehmendem Umfang die Mitgliedsländer zur Erhebung und Verarbeitung personenbezogener Daten — so etwa im Bereich der Landwirtschaftsstatistik — und zur grenzüberschreitenden Datenübermittlung — so beispielsweise im Umwelt-, Gesundheits- und Sozialbereich.

— Einige Länder der Europäischen Gemeinschaft arbeiten an einem Pilot-Projekt für gemeinsame polizeiliche Fahndungsdateien (Schengener Informationssystem) — gewissermaßen als Ersatz für die wegfallenden Kontrollen an den Binnengrenzen.

— Die Einrichtungen der EG selbst führen zunehmend personenbezogene Datenbanken. Diese Einrichtungen unterliegen jedoch keinem Datenschutzgesetz und sind daher nicht an die Grundsätze des Datenschutzes gebunden.

Die Europäische Gemeinschaft und ihre Mitgliedstaaten werden aufgefordert, in ihre Planungen für „Europa '92" die Notwendigkeit eines umfassenden und konsistenten Ansatzes zur Verwirklichung der Grundsätze des Datenschutzes in den Mitgliedsländern und in bezug auf die Aktivitäten der Gemeinschaft selbst einzubeziehen.

Im einzelnen schlägt die Konferenz vor:

— Durch entsprechende Rechtsakte der Europäischen Gemeinschaft sollten die Grundsätze der Europaratskonvention 108 für alle Mitgliedstaaten ebenso wie für die Institutionen der EG selbst verbindlich gemacht werden.

— Eine unabhängige Datenschutzkontrollinstanz sollte eingerichtet werden. Sie sollte die Einrichtungen der EG in allen Datenschutzfragen beraten, die Verarbeitung personenbezogener Daten innerhalb der Einrichtungen der EG kontrollieren, Eingaben von Betroffenen entgegennehmen und mit den nationalen Datenschutzorganen zusammenarbeiten.

Die Commission Nationale de l'Informatique et des Libertés (die französische Datenschutzkommission) wird gebeten, diese Vorschläge alsbald dem Vorsitzenden des Ministerrats sowie den Präsidenten des Europaparlaments und der EG-Kommission zu unterbreiten und um Unterstützung zu werben.

Anlage 13 (zu 1.4, 27.6)

Erklärung zum Datenschutz bei dem von den Unterzeichnerstaaten des Schengener Übereinkommens geplanten gemeinsamen Informationssystem vom 16. März 1989

1. Die nationale Kommission für die Informatik und die Freiheiten (CNIL) der französischen Republik, der Bundesbeauftragte für den Datenschutz der Bundesrepublik Deutschland und die beratende Kommission nach dem Datenschutzgesetz des Großherzogtums Luxemburg vom 31. März 1979 haben über das Vorhaben der Regierungen Frankreichs, der Bundesrepublik Deutschland und den Benelux-Staaten beraten, auf der Grundlage des Schengener Übereinkommens gemeinsame automatisierte Dateien der Polizei einzurichten.

2. Die Datenschutzbeauftragten widersprechen nicht dem Ziel, in einem Europa mit offenen Grenzen die internationale Zusammenarbeit der Polizei durch grenzüberschreitende Informationssysteme zu verbessern. Sie machen aber darauf aufmerksam, daß mit dem geplanten Schengener Informationssystem (S.I.S.) eine neue Dimension der grenzüberschreitenden Verarbeitung personenbezogener Daten bewirkt wird. Sie fordern deshalb, daß zugleich mit der Planung dieses Systems ein wirksamer Datenschutz sichergestellt wird.

3. Diese Forderung ist von essentieller Bedeutung, und zwar aus mehreren Gründen:

   3.1. Das geplante Informationssystem kann die Rechte der Bürger empfindlich treffen. Es dient nicht nur der Ausschreibung von Verdächtigen zur Festnahme, sondern beispielsweise auch der Suche nach Vermißten (auch Minderjährigen) und nach gestohlenen Ausweispapieren, der Ermittlung des Aufenthalts von Personen, der teilweise verdeckten Sammlung von Informationen in allen Bereichen, der Zurückweisung oder Abschiebung unerwünschter Ausländer und der gezielten zollmäßigen Untersuchung beim Grenzübertritt.

   3.2. Einer der Unterzeichnerstaaten des Schengener Übereinkommens hat noch kein Datenschutzgesetz. Zwei weitere haben zwar ein allgemeines Gesetz erlassen, aber noch keine Regelungen für den Polizeibereich.

   3.3. Es ist beabsichtigt, das Schengener Modell später auf alle Mitgliedsländer der Europäischen Gemeinschaften zu erweitern. Gegenwärtig haben aber fünf der zwölf Mitgliedsländer noch kein Datenschutzgesetz.

   3.4. Nach wenigen Jahren kann der Wunsch entstehen, die gemeinsame Datenverarbeitung über die polizeiliche Fahndung hinaus zu erweitern, etwa auf den Erkennungsdienst oder auf Daten über alle Straftaten und Tatverdächtigen sowie auf Haftzeiten.

4. Nach Auffassung der Datenschutzbeauftragten müssen die folgenden Mindestbedingungen erfüllt sein, bevor das S.I.S. in Betrieb genommen wird:

   4.1. Der Inhalt gemeinsamer Dateien, ihr Zweck und ihre Verwendung müssen präzise und abschließend rechtsverbindlich definiert werden.

   4.2. Der Einzelne muß in jedem Vertragsstaat ein Recht auf Zugang zu den ihn betreffenden gespeicherten Daten haben — wobei Einschränkungen aus Gründen der polizeilichen Aufgabenerfüllung in Betracht kommen — und ein Recht auf Berichtigung unzutreffender sowie auf Löschung nicht stichhaltiger Daten haben.

   4.3. Die Verarbeitung und Nutzung der gespeicherten personenbezogenen Daten muß in allen Vertragsstaaten einer Kontrolle durch unabhängige Organe unterliegen.

   4.4. Es ist Aufgabe eines gemeinsamen Organs, daß aus Vertretern der nationalen Kontrollorgane der Vertragsstaaten zusammenzusetzen ist, gemeinsame Kontrollaufgaben wahrzunehmen und insbesondere die Probleme zu erörtern und einer harmonisierten Lösung zuzuführen, die sich aus der Praxis der nationalen Kontrollorgane ergeben können.

   4.5. Ohne der Einrichtung dieses noch zu schaffenden gemeinsamen Organs vorzugreifen, sollten die nationalen Datenschutzkontrollorgane schon jetzt an der Ausarbeitung des S.I.S. beteiligt werden.

   4.6. Die Bestimmungen des Datenschutzübereinkommens des Europarats sind als verbindliche Mindestanforderungen zu betrachten.

5. Auch auf den Gebieten des Ausländerrechts und des Asylrechts wird der Datenaustausch eine neue Dimension erreichen, um gemeinsame Ziele durch abgestimmtes Vorgehen zu erreichen. Die Datenschutzbeauftragten werden auf allen Gebieten darüber wachen, daß neue grenzüberschreitende Datenflüsse und internationale Informationssysteme nur eingerichtet werden, wenn die Mindestanforderungen des Datenschutzes in allen Vertragsstaaten erfüllt sind.

Anlage 14 (zu 27.4)

Entwurf von Richtlinien betreffend personenbezogene Daten in automatisierten Dateien (von der Menschenrechtskommission der Vereinten Nationen am 6. März 1989 beschlossene Fassung, MRK-Resolution 1989/43)

I.

Grundsätze, die einen Mindeststandard festlegen, der bei der nationalen Gesetzgebung berücksichtigt werden sollte

1. *Grundsatz der Rechtmäßigkeit und der Ehrlichkeit:*

Personenbezogene Informationen sollten weder auf unehrliche oder rechtswidrige Weise erhoben oder verarbeitet werden, noch sollten sie für Zwecke verwendet werden, die im Gegensatz zu den Zielsetzungen und Grundsätzen der Charta der Vereinten Nationen stehen.

2. *Grundsatz der Richtigkeit:*

Die für die Zusammenstellung und Führung von Dateien verantwortlichen Personen sind dazu verpflichtet, die Richtigkeit und Relevanz der erfaßten Daten regelmäßig zu überprüfen und dafür Sorge zu tragen, daß sie regelmäßig oder anläßlich der Verwendung der in der Datei gespeicherten Angaben auf den neuesten Stand gebracht werden.

3. *Grundsatz der Zweckbestimmung:*

Der Zweck, für den die Datei verwendet werden soll, sollte genau bestimmt werden, rechtmäßig und öffentlich bekannt sein, bevor sie eingerichtet wird. Dadurch soll anschließend sichergestellt werden können, daß

a) alle erhobenen und erfaßten personenbezogenen Daten für den solcherart festgelegten Zweck relevant und angemessen bleiben

b) keine der genannten personenbezogenen Daten für Zwecke, die im Widerspruch mit den solcherart festgelegten Zwecken stehen, genutzt oder übermittelt werden, es sei denn, der Betroffene hat eingewilligt

c) der Zeitraum, über den die personenbezogenen Daten aufbewahrt bleiben, nicht länger ist als der Zeitraum, der zur Erfüllung des solcherart festgelegten Zwecks erforderlich ist.

4. *Grundsatz der Möglichkeit des Betroffenen zur Einsichtnahme:*

Ungeachtet der Staatsangehörigkeit oder des Wohnortes hat jeder, der seine Identität nachweist, das Recht, Kenntnis davon zu erlangen, ob seine Person betreffende Informationen verarbeitet werden und sie ohne unangemessene Verzögerung oder Kosten in verständlicher Form zur Verfügung gestellt zu bekommen sowie im Falle unrechtmäßiger, nicht erforderlicher oder ungenauer Eintragungen eine entsprechende Berichtigung bzw. Löschung zu erwirken. Entsprechende Rechtsmittel sollten festgelegt werden. Die Kosten einer Berichtigung sind von der für die Datei verantwortlichen Person zu tragen.

5. *Grundsatz der Nichtdiskriminierung:*

Vorbehaltlich der restriktiv im Grundsatz 6 niedergelegten Ausnahmen sollten Daten, die leicht zu ungesetzlicher oder willkürlicher Diskriminierung führen können, insbesondere Angaben über rassische oder ethnische Herkunft, Hautfarbe, Sexualleben, politische Anschauungen, religiöse, weltanschauliche und andere Überzeugungen sowie die Mitgliedschaft in einer Vereinigung oder einer Gewerkschaft, nicht erfaßt werden.

6. *Ausnahmebefugnisse:*

Abweichungen von den unter 1 bis 4 genannten Grundsätzen dürfen nur zugelassen werden, wenn sie erforderlich sind, um die nationale Sicherheit, die öffentliche Ordnung, die öffentliche Gesundheit oder Moral oder die Rechte und Freiheiten anderer, einschließlich verfolgter Personen, zu schützen und durch Gesetz oder entsprechende Regelungen festgelegt sind. Diese Gesetze oder Regelungen müssen, in Übereinstimmung mit der Rechtsordnung des jeweiligen Staates, ausdrücklich die Grenzen dieser Ausnahmen festlegen und einen angemessenen Schutz gewährleisten.

Ausnahmen von dem im Grundsatz 5 verankerten Verbot der Diskriminierung dürfen, abgesehen davon, daß für sie die für Ausnahmen von den Grundsätzen 1 bis 4 vorzusehenden Schutzbestimmungen bestehen müssen, nur zugelassen werden, wenn sie mit der Allgemeinen Erklärung der Menschenrechte und anderen maßgeblichen Rechtsinstrumenten zum Schutz der Menschenrechte und der Verhütung von Diskriminierung vereinbar sind.

7. *Grundsatz der Sicherheit:*

Geeignete Maßnahmen sollten ergriffen werden, um die Dateien sowohl gegen Naturgefahren, wie

zufälligen Verlust oder Zerstörung, als auch gegen Gefahren durch menschliche Einwirkungen, wie unerlaubten Zugang oder vorsätzlichen Mißbrauch von Daten, zu schützen.

8. *Überwachung und Sanktionen:*

   Im Gesetz des jeweiligen Landes ist festzulegen, welche Stelle in Übereinstimmung mit der Rechtsordnung des jeweiligen Staates dafür zuständig sein soll, die Einhaltung der obigen Grundsätze zu überwachen. Diese Stelle muß Garantien für Unparteilichkeit und fachliche Kompetenz bieten. Für den Fall der Verletzung der nationalen Rechtsvorschriften, die zur Verwirklichung der vorgenannten Prinzipien geschaffen worden sind, sollten Kriminalstrafen und angemessene Rechtsmittel vorgesehen werden.

9. *Grenzüberschreitender Datenverkehr:*

   Sofern bei einem grenzüberschreitenden Datenverkehr die Gesetzgebungen zweier oder mehrerer betroffener Staaten mehr oder weniger gleichwertige Sicherungen für den Schutz der Privatsphäre bieten, sollten die Informationen zwischen ihnen so frei wie innerhalb jedes Einzelstaates ausgetauscht werden können. Wenn keine gegenseitigen Schutzbestimmungen bestehen, dürfen Beschränkungen für diesen Austausch nicht unangemessen und nur insoweit zulässig sein als der Schutz der Privatsphäre es erfordert.

10. *Geltungsbereich:*

    Die obigen Bestimmungen sollten in erster Linie für alle öffentlichen und privaten automatisierten Dateien gelten einschließlich manueller Dateien, für die diese Bestimmungen unter dem Vorbehalt entsprechender Anpassungen Gültigkeit haben sollten.

    Zusätzlich sollten bei Bedarf spezielle Bestimmungen geschaffen werden, wodurch alle oder ein Teil der Grundsätze auch für Dateien über juristische Personen gelten sollen, wenn diese Angaben über Einzelpersonen enthalten.

II.

Anwendung der Richtlinien auf personenbezogene Daten in den Dateien internationaler staatlicher Organisationen

Die vorliegenden Richtlinien sollten für personenbezogene Daten in Dateien staatlicher internationaler Organisationen gelten, vorbehaltlich etwa erforderlicher Anpassungen in Bezug auf eventuelle Unterschiede zwischen internen Dateien betreffend Personal sowie vergleichbare Gruppen und externen Dateien, die sich auf Dritte beziehen, welche mit der Organisation in Verbindung stehen.

Eine Abweichung von diesen Prinzipien kann für Dateien vorgesehen werden (humanitärer Vorbehalt), deren Zweck auf den Schutz der Menschenrechte und Grundfreiheiten des einzelnen oder humanitären Beistand gerichtet ist.

Jede Organisation sollte eine Behörde benennen, die eine gesetzliche Zuständigkeit für die Überwachung der Einhaltung dieser Regelungen besitzt.

Eine entsprechende Bestimmung sollte in der nationalen Gesetzgebung für die nicht-staatlichen internationalen Organisationen, für welche dieses Gesetz Anwendung findet, vorgesehen werden sowie für die staatlichen internationalen Organisationen, deren Abkommen über den Sitz der Organisation nicht die Anwendung der genannten nationalen Gesetzgebung ausschließt.

Sachregister

Abkürzungsverzeichnis

AA	Auswärtiges Amt
ADOS	Adressen und Objekte Ost
AFG	Arbeitsförderungsgesetz
AIDS	Acquired Immune Deficiency Syndrome
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
APIS	Arbeitsdatei PIOS innere Sicherheit
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
BA	Bundesanstalt für Arbeit
BABSY	Beihilfeabrechnungssystem
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesarbeitsgericht
BASt	Bundesanstalt für Straßenwesen
BAW	Bundesanstalt für Wirtschaft
BAZ	Bundesamt für den Zivildienst
BDSG	Bundesdatenschutz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BKA	Bundeskriminalamt
BMA	Bundesminister für Arbeit und Sozialordnung
BMBau	Bundesminister für Raumordnung, Bauwesen und Städtebau
BMBW	Bundesminister für Bildung und Wissenschaft
BMF	Bundesminister der Finanzen
BMI	Bundesminister des Innern
BMJ	Bundesminister der Justiz
BMJFFG	Bundesminister für Jugend, Familie, Frauen und Gesundheit
BML	Bundesminister für Ernährung, Landwirtschaft und Forsten
BMP	Bundesminister für das Post- und Fernmeldewesen
BMPT	Bundesminister für Post und Telekommunikation
BMU	Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BMWi	Bundesminister für Wirtschaft
BND	Bundesnachrichtendienst
BNDG	Bundesnachrichtendienst-Gesetz
BPersVG	Bundespersonalvertretungsgesetz
BRH	Bundesrechnungshof
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfSchG	Bundesverfassungsschutzgesetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
coArb	computerunterstützte Arbeitsverwaltung
coLei	computerunterstützte Leistungsgewährung
COMPAS	computerunterstütztes Ausbildungsvermittlungssystem
DBP	Deutsche Bundespost
DNA	Desoxyribonucleinacid
DV/dv	Datenverarbeitung

EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
FRV	Fahrzeugregisterverordnung
G 10	Gesetz zur Beschränkung der Brief-, Post- und Fernmeldegeheimnisse
GG	Grundgesetz
GMBl	Gemeinsames Ministerialblatt
GRG	Gesundheits-Reformgesetz
HGB	Handelsgesetzbuch
HIV	Human Immundeficiency Virus
INPOL	Informationssystem der Polizei
ISDN	Integrates Services Digital Network
ISIT	Interministerieller Ausschuß für die Sicherheit in der Informationstechnik
IT	Informationstechnik
KBA	Kraftfahrt-Bundesamt
LVA	Landesversicherungsanstalt
LBA	Luftfahrt-Bundesamt
MAD	Militärischer Abschirmdienst
MADG	Militärischer Abschirmdienst-Gesetz
MRRG	Melderechtsrahmengesetz
MS-DOS	Microsoft Disc Operating System
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenzeitschrift
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
PC	Personalcomputer
PDV	Polizeidienstvorschrift
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PostG	Postgesetz
PSV	Psychologische Verteidigung
Reha	Rehabilitation
RRG	Rentenreformgesetz
RVO	Reichsversicherungsordnung
SAP	Sozialamt der Deutschen Bundespost
SGB I	Sozialgesetzbuch Erstes Buch
SGB X	Sozialgesetzbuch Zehntes Buch
S.I.S.	Schengener Informationssystem
SPUDOK	Spurendokumentationssystem
StDAV	Steuerdaten-Abruf-Verordnung
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht *)
TEMEX	Telemetry Exchange

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erscheinen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/4690
Neunter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 10/6816
Zehnter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 11/1693
Elfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache 11/3932

THW	Technisches Hilfswerk
TKO	Telekommunikationsordnung
VAP	Versorgungsanstalt der Deutschen Bundespost
VDR	Verband der Rentenversicherungsträger
VwGO	Verwaltungsgerichtsordnung
VZR	Verkehrszentralregister
WEWIS	Wehrersatzwesen-Informationssystem
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung



Druck: Bonner Universitäts-Buchdruckerei, 5300 Bonn
Alleinvertrieb: Verlag Dr. Hans Heger, Postfach 20 13 63, Herderstraße 56, 5300 Bonn 2, Telefon 02 28/36 35 51, Telefax 02 28/36 12 75
ISSN 0722-8333